An Engineering Study of
Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME III: ELECTRICAL POWER

CR 115259

Huntsville

IBM

An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME III: ELECTRICAL POWER

IBM NUMBER: 71W-00310

SEPTEMBER 1971

Prepared for the
National Aeronautics and Space Administration
Manned Spacecraft Center
Houston, Texas 77058

CONTRACT NUMBER NAS9-11189

IBM Federal Systems Division, Electronics Systems Center/Huntsville, Alabama

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

FOREWORD

This is one of a set of seven reports, each one describing the results, for a particular subsystem, of a study titled "An Engineering Study of Onboard Checkout Techniques." Under the general title of "A Guide to Onboard Checkout," the reports are as follows.

Volume	IBM Number	Subsystem
I	71W-00308	Guidance, Navigation and Control
II	71W-00309	Environmental Control and Life Support
III	71W-00310	Electrical Power
IV	71W-00311	Propulsion
V	71W-00312	Data Management
VI	71W-00313	Structures/Mechanical
VII	71W-00314	R.F. Communications

This set of guides was prepared from the results of a nine month "Engineering Study of Onboard Checkout Techniques" (NAS9-11189) performed under NASA contract by the IBM Federal Systems Division at its Space Systems facility in Huntsville, Alabama, with the support of the McDonnell Douglas Astronautics Company Western Division, Huntington Beach, California.

Technical monitor for the study was Mr. L. Marion Pringle, Jr. of the NASA Manned Spacecraft Center. The guidance and support given to the study by him and by other NASA personnel are gratefully acknowledged.

Section 1

INTRODUCTION

1.1 OBJECTIVE

With the advent of large scale aerospace systems, designers have recognized the importance of specifying and meeting design requirements additional to the classical functional and environmental requirements. These "additional" requirements include producibility, safety, reliability, quality, and maintainability. These criteria have been identified, grown into prominence, and become disciplines in their own right. Presently, it is inconceivable that any aerospace system/ equipment design requirements would be formulated without consideration of these criteria.

The complexity, sophistication and duration of future manned space missions demand that still another criterion needs to be considered in the formulation of system/equipment requirements. The concept of "checkoutability" denotes the adaptability of a system, subsystem, or equipment to a controlled checkout process. As with other requirements, it should also apply from the time of early design concept formulation.

The results of "An Engineering Study of Onboard Checkout Techniques" and other studies indicate that for an extended space mission onboard checkout is mandatory and applicable to all subsystems of the space system. In order to use it effectively, "checkoutability" should be incorporated into the design of each subsystem, beginning with initial performance requirements.

Conferences with researchers, system engineers and subsystem specialists in the course of the basic Onboard Checkout Techniques Study revealed an extensive interest in the idea of autonomous onboard checkout. Designers are motivated to incorporate "checkoutability" into their subsystem designs but express a need for information and guidance that will enable them to do so efficiently.

It is the objective of this report to present the results of the basic study as they relate to one space subsystem to serve as a guide, by example, to those who in the future need to implement onboard checkout in a similar subsystem. It is not practicable to formulate a firm set of instructions or recipes, because operational requirements, which vary widely among systems, normally determine the checkout philosophy. It is suggested that the reader study this report as a basis from which to build his own approach to "checkoutability."

1.2 BASIC STUDY SUMMARY

1.2.1 STUDY OBJECTIVE

The basic study was aimed at identification and evaluation of techniques for achieving the following capabilities in the operational Space Station/Base, under control of the Data Management System (DMS), with minimal crew intervention.

- Automated failure prediction and detection
- Automated fault isolation
- Failure correction
- Onboard electronic maintenance

1.2.2 STUDY BASELINE

The study started in July 1970. The system design baseline was established by the Space Station Phase B study results as achieved by the McDonnell-Douglas/ IBM team, modified in accordance with technical direction from NASA-MSC. The overall system configuration was the 33-foot diameter, four-deck, 12-man station. Individual subsystem baseline descriptions are given in their respective "Guide to Onboard Checkout" reports.

1.2.3 STUDY TASKS

The basic study comprised five tasks. Primary emphasis was given to Task 1, Requirements Analysis and Concepts. This task established subsystem baseline descriptions and then analyzed them to determine their reliability/maintainability characteristics (criticality, failure modes and effects, maintenance concepts and line replaceable unit (LRU) definitions), checkout strategies, test definitions, and definitions of stimuli and measurements. After software preliminary designs were available, an analysis of checkout requirements on the DMS was performed.

A software task was performed to determine the software requirements dictated by the results of Task 1.

Task 3 was a study of onboard electronic maintenance requirements and recommendations of concepts to satisfy them. Supporting research and technology tasks leading to an onboard maintenance capability were identified. The study implementation plan and recommendations for implementing results of the study were developed in Task 4. The task final report also summarizes results of the study in all technical tasks.

Reliability, Task 5, was very limited in scope, resulting in an analysis of failure modes and effects in three Space Station subsystems, GN&C, DMS (computer group) and RF communications.

1.2.4 PREVIOUS REPORTS

Results of the basic study were reported by task in the following reports, under the general title of "An Engineering Study of Onboard Checkout Techniques, Final Report."

IBM Number	Title
71W-00111	Task 1: Requirements Analysis and Concepts
71W-00112	Task 2: Software
71W-00113	Task 3: Onboard Maintenance
71W-00114	Task 4: Summary and Recommendations
71W-00115	Task 5: Subsystem Level Failure Modes and Effects

Section 2

BASELINE SUBSYSTEM DESCRIPTIONS

2.1 GENERAL

This section describes the baseline Electrical Power Subsystem which was analyzed to define onboard checkout requirements. In order to assess requirements for onboard checkout, descriptions at the subsystem level and the assembly level are required, as well as the major interfaces between subsystems.

The assembly level description for each of the subsystems (MSFC-DRL-160, Line Item 13) provided the primary working document for subsystem analysis. To reduce documentation, these documents have been incorporated by reference into this report, where applicable. Therefore, where no significant differences exist from the Phase B definition, this report contains a brief subsystem description and an identification of the referenced document containing the assembly level descriptions for that subsystem. Where significant differences do exist, the subsystem level description includes these changes in as much detail as is available. MSFC-DRL-160, Line Item 19, provided the major subsystem interface descriptions for analysis of integrated test requirements.

2.2 SUBSYSTEM LEVEL DESCRIPTION

The function of the Electrical Power Subsystem is to generate, condition, control, and distribute electrical power to the Space Station power-consuming subsystems.

This section describes the isotope/Brayton cycle EPS and specifies its characteristics, design parameters, and overall performance.

The Electrical Power Subsystem consists of four major subassembly groups:

- Power Source Assembly Group
- Energy Storage Assembly
- Power System Management Assembly
- Transmission/Conditioning/Distribution Assembly Group

The Isotope/Brayton Power System employs radiative transfer from the isotope heat source array to the Brayton cycle heat exchanger. This arrangement permits Power Conversion System (PCS) module replacement without cutting high temperature lines. The central element is the PCS-heat exchanger module, which has been designed not only for long system lifetime, but also to allow rapid changeout of a failed module.

The output of the power source assembly group is 29.8 kWe of 1200-Hz, 120/208-vac, three-phase electrical power, with 14.9 kWe provided by each PCS. The electrical power is delivered to separate source buses, which represent the initial elements of the transmission, conditioning, and distribution assembly group.

The energy storage assembly provides stored energy for following the variable vehicle power loading while maintaining constant Brayton cycle power loading, provides emergency power for a minimum of 1 hour for crew escape or Station reactivation, and provides initial power for Station activation.

The power management assembly provides control and display functions for all EPS assemblies and interfaces with the Central Control Stations, the Data Management Subsystem, and the Onboard Checkout System.

In addition to the 29.8 kWe total of electrical power, which corresponds to 25 kWe average available at the ac and dc load buses, 4.0 kWt of thermal power (2.0 kWt from each heat source) is extracted as waste heat at 250^{o}F for use by the EC/LS Subsystem. Consequently, the equivalent rating of the I/Br EPS is 25 kWe plus 4 kWe, or 29 kW at the load buses. This performance is uniquely available from this system.

The heat source is a Pu-238 isotope IRV radiantly coupled to a Brayton Cycle Conversion System generating 14.9 kWe at the alternator terminals after losses for PCS control, monitoring, and pumping.

Thermodynamic energy not converted to electricity is transferred from the Xe-He Brayton cycle working fluid to a recirculating FC-75 liquid radiator loop through a heat rejection heat exchanger. The mechanical losses of the Combined Rotating Unit (CRU) and the generator losses are transferred to a parallel cooling loop through a separate heat exchanger.

Conversion of thermal power to electrical power is performed by a recuperated Brayton cycle loop using a single-shaft CRU with a Rice alternator operating at 36,000 rpm. The indicated performance and state point conditions are established by the operating temperature ratio (heat sink heat exchanger temperature versus heat source heat exchanger temperature), and the projected PCS performance is based on extrapolation of Brayton B engine test data. PCS parasitic losses (pump and electrical power control) are deducted from the alternator output. The overall system efficiency of 25.8 percent is based on isotope heat production (end-of-life) and power available at the electrical load bus for subsystems and experiments.

2.3 ASSEMBLY LEVEL DESCRIPTION

Descriptions of the Electrical Power Subsystem assembly groups and assemblies are provided in the Space Station MSFC-DRL-160, Line Item 13, Volume I, Book 1, Electrical Power. These descriptions include discussions of the assembly groups and assemblies, physical characteristics, block diagrams and drawings, and design characteristics. DRL 13, Volume I, Book 2, is incorporated by reference into this report as a detailed description of the Electrical Power Subsystem assembly groups and assemblies and will become the primary working document for further analysis.

Section 3

RELIABILITY AND MAINTAINABILITY ANALYSES

3.1 CRITICALITY ANALYSIS

As a guide to emphasis in subsequent checkout technique studies, an analysis has been made of the overall subsystem and major component criticality (failure probability) of the Space Station subsystems and equipment. As an input to the Checkout Requirements Analysis Task, this data along with the failure mode and effects data will be useful in determining test priorities and test scheduling. Additionally, this data will aid in optimizing checkout system design to ensure that confidence of failure detection is increased in proportion to added system complexity and cost.

3.1.1 CRITICALITY ANALYSIS PROCEDURE

A criticality number (related to failure probability) was generated for each major subsystem component. This number is the product of: (1) the component failure rate (or the reciprocal of mean-time-between-failure), (2) the component's anticipated usage or duty cycle, and (3) an orbital time period of six months, or 4,380 hours. Six months was chosen as the time period of interest to allow one missed resupply on the basis of normal resupply occurring at three-month intervals. The criticality number, then, is the failure expectation for a particular component over any six-month time period.

For visibility, the major components of each subsystem analyzed have been ordered according to the magnitude of their criticality numbers. This number, however, should not be considered as an indication of the real risk involved, since it does not take into account such factors as redundant components, subsystem maintainability, and the alternate operational procedures available.

Overall subsystem criticality has been determined by a computerized optimization process whereby spares and redundancy are considered in terms of a trade-off between increased reliability and weight. This determination, therefore, reflects not only the failure probability of subsystem components, but also the probability that a spare or redundant component may not be available to restore the subsystem to operational status. The methodology used is described in Section 9, Long-Life Assurance Study Results, DRL 13 (Preliminary Subsystem Design Data), Volume III (Supporting Analyses), Book 4 (Safety/Long Life/Test Philosophy) from the MDAC Phase B Space Station Study. Component-level failure mode and criticality data are presented in subsequent paragraphs.

3.1.2 ELECTRICAL POWER

The optimized six-month reliability for the Electrical Power Subsystem (EPS) is 0.997 and requires 1,300 pounds of spares for its achievement. An ordered ranking of EPS component criticality is provided in Table 3-1.

3.2 FAILURE EFFECTS ANALYSIS

Based upon the baseline subsystem descriptions, each major subsystem component was assessed to determine its most probable failure mode(s), and the "mission effect" associated with this failure mode(s). The "mission effect" is noted to provide a brief explanation of Space Station behavior if the particular failure mode should occur (e.g., experiments degraded, crew hazard, etc.). The explanation generally does not consider the offsetting effects of backup redundancy or spares since there would be practically no effect if these factors were considered.

In addition, the effect of failure is categorized into the following criticality classes:

(a) Category I - Failure could cause a loss of life.

(b) Category II - Failure could cause the loss of a primary mission objective.

(c) Category III - Failure could cause the loss of a secondary mission objective.

(d) Category IV - Failure results in only a nuisance.

In most cases, Category II and Category III failures are not distinguishable because primary and secondary mission objectives have not been identified to the level of detail required to permit such separation.

The EPS failure mode analysis deviates somewhat from that conducted on other subsystems. This was necessary because many failures will only cause temporary loss of up to 12.5 kw, and then only if the batteries were not fully charged. For this reason the "mission effects" column presents the actual effects on the total EPS system, considering backup. Most failures are placed in Category II which means that experiments could be temporarily curtailed if repair is not accomplished in a reasonable time.

Table 3-2 presents a partial listing of failure modes and criticality classification data which should serve as a useful example.

Table 3-1. Electrical Power Criticality Ranking

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
Heat Rejection System	132,000	1,750	Backup heat rejection system. Includes failure to start up, four primary and four secondary radiator loops and two are standby
1.3 kW Sine Wave Inverter	47,000	220	Standby unit on line. Internal short can be cleared. Circuit breaker trips
1.0 kW Sine Wave Inverter	47,000	<10	Same as 1.3 kW 400 H_3 inverter plus emergency inverter backup
5.8 kW Square Wave Inverter	47,000	220	Standby unit on line. Circuit breaker will trip against overload
Power Conversion Loop	45,500	500	One standby spare PCS reduces criticality to 5000. Ability to switch on batteries and/or tolerate 1/2 power should reduce criticality to 500
IRV Heat Source	16,700	40	S/S batteries pushing up load could reduce criticality as shown for up to 24 hours or until new heat source was obtained. Must resort to heat dump mode utilizing quad redundant springs, bi-redundant hinges, to reduce crew hazard
Battery Chargers	4,700	<10	Includes backup charger plus extended capability to operate without battery recharge until new charger resupplied
Regulated Hi Voltage Rectifier	2,630	25	Includes partial loss of redundancy

Table 3-1. Electrical Power Criticality Ranking (Continued)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
5 kW Regulated X frm/Rectifier	1,800	2	For "fail open", output is sensed, failed unit isolated, and standby unit brought on line. Internal short is cleared by reverse current relay in output and circuit breaker in input
Batteries	1,100	<10	Spare battery available plus modules. Can curtail experiments requiring peak power. Batteries are double contained (sealed to prevent KOH leakage)
All Other Components		<10	

Table 3-2. EPS Subsystem

Major Subsystem Component	Failure Mode(s)	Mission Effect	Failure Category	No. of Units	(A) MTBF/Source Thousands of Hours	(B) Duty Cycle (%)	Criticality Unit (4380 hrs X B/A X 10^{-6})
1) Alternate Feeder/Source Bus	Short Open Phase	Loss of 1/2 source capacity until faulted feeder is replaced	II	2	----	100	Neg'l
2) Source Bus Parallel Feeder	Short Open Phase	Loss of faulted feeder; redundant feeder utilized and spare replaces faulted feeder	II	4	----	100	Neg'l
3) Transmission Circuits (Deck 3 to Deck 1)	Short Open Phase	Must switch to alternate circuit	II	2	----	100	Neg'l
4) 5 kw Regulated X fmr/Rectifier	Open/short	Loss of redundancy but not load; only critical if standby unit cannot be brought on line	II	4	2,460/(2)	100	1,800
5) 1.3 kw Sine Wave Inverter	Open/short	Momentary loss of all 400 Hz sine wave power until standby unit switched in	II	1	94./(4)	100	47,000
6) 1.0 kw Sine Wave Inverter	Open/short	Same as No. 5 for 6 OH_Z power	II	1	94./(4)	100	47,000
7) Regulated Hi-Voltage Rectifiers	Open/short	Curtailment of some load requiring 400 Hz until redundant unit switched in	II	2	1,660	100	2,630

3.3 MAINTENANCE CONCEPT ANALYSIS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment.

3.3.1 GENERAL CONSIDERATIONS

General considerations governing maintenance philosophy in the Space Station are discussed in Section 7. Specific applications to the Electrical Power Subsystem are discussed in the next subsection.

3.3.2 EPS MAINTENANCE

The major maintenance activity for the Electrical Power Subsystem is associated with circuit breakers, switches, inverters, battery chargers, voltage regulators, etc. These are replaceable items, and also contain replaceable function modules, such as electronic circuit cards. Provisions are made for switching in spare voltage regulators, battery chargers, etc., to permit maintenance or replacement at connector plugs as required, except where flat wire circuits are used in consoles. The inverters, voltage regulators and battery chargers are bolted to cold plates using allen-head-type bolts and will require closely-controlled flat surfaces for contact to assure heat transfer.

Two spare power conversion systems (PCS) for the two operating PCSs of the Isotope/Brayton Electrical Power System are installed in the power module (part of the core module), along with the remote handling mechanisms, carriages, and closed circuit TV viewing links used for transferring the PCS during installation or interchange. The PCS has a 2 1/2-year design life. PCS exchange can be performed either remotely or locally; however, work in this unpressurized compartment must be accomplished in a space suit. The isotope reentry vehicle, including the heat source (HS), must be placed in the passive heat dump mode for dissipation of HS energy to space during the PCS transfer. IRV deployment for heat dumping is accomplished by rotation of the IRV hinge mechanism and IRV support ring out of the Space Station port and away from the heat source heat exchanger (HSHX) into a position 90 degrees (or more) away from the radiator in which it is cooled by radiation to space. The IRV/heat source is held in operating position by solenoid-operated shear pins which are positively retracted during the deployment sequence. (Subsequent to launch if PCS power is lost, the pins fail in a retracted position.)

In the event of an abort or to release the IRV and heat source from the Space Station for recovery, the shear pins are first released and the IRV/heat source is moved to the deployed position by preloaded springs. Then the IRV/heat source is removed from the Space Station at the hinge attachment to the support ring, using a number of explosive (squib-actuated) nuts.

When normal recovery by an advanced logistic system is to be accomplished, a remote manipulator on the Crew Cargo/Tug Module will extract the deployed IRV/heat source from the mounting and transfer it, first to the recovery support cradle, and then to the ALS cargo door opening while still contained within the recovery support cradle. All operations will be conducted to incur minimum exposure to the crew from the unshielded IRV/heat source, using remotely controlled manipulators and closed circuit TV observation.

3.4 LINE REPLACEABLE UNIT ANALYSIS

General guidelines and criteria for the definition of LRUs were established and these along with the maintenance philosophies reported in Section 7 were used to determine at what level line maintenance would be performed. For the Space Station Subsystems specific justification applicable to LRU selection for the particular subsystem under examination was derived from the guidelines and these justifications are presented along with the LRU listing. The "functional LRUs" were then considered in the light of the standard electronic packaging scheme and actual LRUs were defined and listed. The method employed and the results achieved are discussed in the following sections.

3.4.1 SPACE STATION SUBSYSTEMS

The definition of Line Replaceable Units (LRUs) is keyed to repairing subsystems in an in-place configuration with the LRU being the smallest modular unit suitable for replacement. General factors considered in identifying subsystem LRUs include: (1) maintenance concepts developed and defined in Section 3.3; (2) the component-level failure rates delineated in the criticality analyses of Section 3.1; (3) the amount of crew time and skill required for fault isolation and repair; (4) resultant DMS hardware and software complexity; and (5) subsystem weight, volume, location, and interchangeability characteristics. Listings of LRUs and more specific justification for their selection follows.

Discussion of the LRUs identified for the Electrical Power Subsystem (EPS) is divided into two parts. The first is concerned with EPS transmission, conditioning, and distribution equipment, while the second addresses the Isotope/Brayton System.

3.4.1.1 Transmission, Conditioning, and Distribution

The EPS transmission/conditioning/distribution (T/C/D) LRUs are listed in Table 3-3 and consist of conductors, conductor terminations, relays, circuit breakers, limiters (fuses), power conditioners, and power control and instrumentation elements.

Table 3-3. Electrical Power Transmission/Conditioning/Distribution

LRU	Quantity Required	Quantity Redundant
Alternator Feeders	2	2
Alternator Feeder Circuit Breakers	2	-
Alternator Feeder/Source Bus Differential Protection Relays	6	-
Alternator Feeder/Source Bus Phase - Balance Protection Relays	2	-
Source Bus to Distributor - No. 2 1200 Hz Transmission Cables	2	2(2)
Distributor No. 2 to Distributor No. 1 - 1200 Hz Transmission Cables	2	1(1)
1200 Hz Transmission Cable Differential Protection Relays	12	-
1200 Hz Transmission Cable Phase-Balance Protection Relays	4	-
1200 Hz Transmission Cable Current Breakers	8	-
1200 Hz Transmission Cable Power Switches	2	-
1200 Hz Transmission Cable Limiters (Fuses)	6	-
Main 1200 Hz Distributor Bus Differential Protection Relays	12	-
Main 1200 Hz Distributor Bus Phase-Balance Protection Relays	2(2)	-
Main 1200 Hz Distributor Bus Power Switches	5	-
Main 1200 Hz Distributor Bus Selector Switches	3	-
Main 1200 Hz Distributor Bus Circuit Breakers	17	3
1200 Hz Feeders to Distribution Panels (Load Buses)	2	2
1200 Hz Distribution Feeder Circuit Breakers	2	2
1200 Hz Load Line Circuit Breakers	$\simeq$10	-
Main 28 Vdc Distributor Differential Protection Relays	4	-

Table 3-3. Electrical Power Transmission/Conditioning/Distribution (Continued)

LRU	Quantity	
	Required	Redundant
Main 28 Vdc Distributor Bus Sectionalizing CBs	2	-
Main 28 Vdc Distributor Bus Power Switches	12	2[4]
Main 28 Vdc Distributor Bus Reverse Current Relays	12	2[4]
28 Vdc Bus Tie Cable	1	1[1]
28 Vdc Bus Tie Cable Circuit Breakers	2	-
28 Vdc Feeders to Distribution Panels (Load Buses)	10	8[4]
28 Vdc Distribution Feeder Circuit Breakers	10	8[4]
28 Vdc Load Line Circuit Breakers	$\simeq$500	$\simeq$75 for essential loads only
260 Vdc Link Bus Differential Protection Relays	2	-
260 Vdc Link Bus Circuit Breakers	3	3[4]
260 Vdc Link Bus Power Switches	2	2[4]
260 Vdc Link Bus Reverse Current Relays	2	2[4]
260 Vdc Bus Tie Cable	1	1[1]
260 Vdc Bus Tie Cable Circuit Breakers	2	-
Main 400 Hz Distributor Bus Power Switches	6[5]	2[5]
400 Hz Square Wave Bus Tie Cable	1	1
400 Hz Square Wave Bus Tie Cable Circuit Breakers	2	-
400 Hz Square Wave Feeders to Distribution Panels	12	4[4]
400 Hz Square Wave Distribution Feeder Circuit Breakers	12	4[4]
400 Hz Square Wave Load Line Circuit Breakers	$\simeq$25	$\sim$20
400 Hz Sine Wave Bus Tie Cable	1	1[1]

Table 3-3. Electrical Power Transmission/Conditioning/Distribution (Continued)

LRU	Quantity	
	Required	Redundant
400 Hz Sine Wave Bus Tie Cable Circuit Breakers	2	-
400 Hz Sine Wave Feeders to Distribution Panels	12	4[4]
400 Hz Sine Wave Distribution Feeder Circuit Breakers	12	4[4]
400 Hz Sine Wave Load Line Circuit Breakers	$\simeq$25	$\sim$20
Main 60 Hz Distributor Bus Power Switches (Single Pole)	2	-
60 Hz Bus Tie Cable (Single Phase)	1	1[1]
60 Hz Bus Tie Cable Circuit Breaker (Single Pole)	1	-
60 Hz Feeders to Distribution Panel (GPL Only)	1	1[2]
60 Hz Distribution Feeder Circuit Breakers (GPL Only)	$\simeq$10	-
60 Hz Bus Sectionalizing and Load Line CBs (GPL Only)	$\simeq$10	-
600 Hz Starting Bus Circuit Breakers (Interlocked)	1	2
600 Hz Starting Bus Selector Switch	1	1
600 Hz Transmission Cable from M-G in Distribution Center No. 1 to Starting Bus in Distributor Center No. 2	1	0
600 Hz Transmission Cable to Alternator No. 1	1	0
600 Hz Transmission Cable to Alternator No. 2	1	0
600 Hz Motor Generator (M-G) Set	1	1
Motor-Generator Input CBs (28 Vdc)	1	1
Regulated Transformer-Rectifiers (28 Vdc)	4	1 [4] [6]
High-Voltage Rectifier Regulator (260 Vdc)	2	2 [4] [6]
400 Hz Square Wave Inverter	1	1 [4] [6]
400 Hz Sine Wave Inverter	1	1 [4] [6]
60 Hz Sine Wave Inverter (Single Phase)	1	1 [4] [6]

Table 3-3. Electrical Power Transmission/Conditioning/Distribution (Continued)

LRU	Quantity	
	Required	Redundant
Launch and Ascent/Emergency Inverter (400 Hz Sine Wave)	1	1 (6)
Launch and Ascent/Emergency Inverter Input CBs (28 Vdc)	1	1
Battery Charger Regulator	10	
Battery	10	
Battery Switching Unit	10	
Buck Regulator (Regulates battery discharge voltage)	10	
Battery Emergency Override Control Circuit Breaker	10	
Power Control Modules (Power Management Assembly)	TBD	TBD
Instrumentation Sensors	TBD	TBD
Signal Conditioning Units	TBD	TBD

(1) Laid-in spare
(2) Operating redundancy
(3) Bus No. 2 only
(4) Standby redundancy
(5) Combined requirements for 400 Hz sine wave and square wave buses. Includes two square wave sine wave bus tie switches interlocked with outputs of emergency inverters.
(6) LRU may be at the component level in the noted modules.

Main ac power feeder circuits are comprised of individual 4-conductor cables having relatively large cross-sectional areas. Both single-cable and multiple-cable circuits are employed. Spare cables complete with terminations are laid in place ready for connection into selected circuits in the event of a conductor/cable failure. This minimizes handling of large-gauge conductors and limits subsystem down time to the affected power circuit.

Differential and reverse current relays, circuit breakers, and switches (either electromechanical or solid state) are multiple usage items installed in panels and other higher-level bussing assemblies. They are selected as LRUs to reduce spares requirements and to minimize load circuit interruptions or power curtailment for either scheduled or unscheduled replacements.

Power conditioners (transformer-rectifiers, inverters, buck regulators, etc.) are typically "black box" end items. On-line redundancy is employed in the operation of these units. The T/C/D system is designed to permit quick replacement of these items in order to maintain operating redundancy/system reliability at required levels.

The design of power conditioning equipment generally lends itself to modularization and fault detection to the module level. Replacement of modules within power conditioners should be considered as an alternate to the "black box" LRU level where module commonality would permit economies-in-spares provisioning.

Typical LRUs for T/C/D instrumentation include sensors and signal conditioners for status display and power protection and control. The uniqueness of many T/C/D sensing devices in terms of location and rating (e.g., current transformers in transmission circuits, as well as distribution circuits, with primary ratings ranging from over 50 amperes to less than 1 ampere) establish these items as LRUs. Selected logic, amplification and possibly computational modules associated with power control are also candidate LRUs.

3.4.1.2 Isotope/Brayton LRUs

A listing of the isotope/Brayton LRUs is given in Table 3-4. Their selection is predicated on nuclear safety, life, and reliability considerations. They are also restricted to those assemblies and components which are readily replaceable and which are within the purview of projected crew skills and available tooling.

Isotope recovery requirements for nuclear safety dictate that the complete isotope reentry vehicle (IRV) heat source assembly be a line replaceable unit. Radiation hazard prevents any subassembly or component within the IRV heat source from being replaced. Therefore, all critical components and instrumentation are installed with adequate on-line and standby redundancy or alternate modes of operation to provide acceptable performance for the life of the IRV heat source. Typical examples are: (1) the dual hinges that allow the IRV heat

Table 3-4. Electrical Power Isotope/Brayton System

LRU	Quantity Required	Quantity Standby Redundant
Isotope Reentry Vehicle Heat Source	2	
Power Conversion System	2	1
Solenoid Valve Electrical Assembly	12	6
Insulation	-	
Surface Thermocouple	26	13
Mounting Attachment	TBD	TBD
Heat Rejection System		
Pump Motor	8	
Transducers	44	
Cold Plate	6	
Diversion Valve	8	
Pump Motor Electrical Switch	8	
Insulation	-	
Gas Management System		
Heater Contactor	2	
Gas Storage Bottle	2	
Transducer	4	
Solenoid Valve Electrical Assembly	10	
Electronic Monitoring and Control Assembly		
Signal Conditioner Module	2	1
Speed Control and Dissipative Load Bank Unit	2	1
Voltage Regulator Exciter	2	1
Shield Assembly		
Shield	2	
Shield Retraction Cable	2	
Shield Retraction Sheave	2	
Shield Retraction Drive	2	

source to open on either side for emergency cooling; and (2) the critical heat source temperature instrumentation having triple redundant sensors at both the capsule and on the BeO heat sink.

The Brayton Power Conversion System (PCS) is hermetically sealed for operation in the space environment. The complete PCS is replaceable as well as those PCS components that do not require the opening of working fluid lines. Replaceable components are therefore limited to surface thermocouples, solenoid valve electrical assemblies, and mounting fixtures. Replacement of internal components; e.g., rotating unit, heat exchangers, pressure gauges, and valve bodies, would require cutting and welding lines that operate at high temperatures and pressure. Extensive inspection, testing, and gas recharging would also be required before the system could be put back on-line. Attendant skills, tooling, and gas management capacity are not available in the baseline system to allow replacement at this level.

Unitized construction of the cooling tubes, meteoroid bumpers, and spacecraft structure as well as the length of radiator cooling tubes preclude classifying the Heat Rejection System as a line replaceable unit. In view of this, all components of the Heat Rejection System (e.g., sensors, pumps), with the exception of the radiator tubes, are made line replaceable. In addition, extensive redundancy is employed in the baseline system because of the complexity of removal and replacement of heat rejection components.

Gas Management System components are replaceable if they are upstream of the solenoid valves that isolate this system from the PCS. The jacking gas supply is paralleled with the second onboard Gas Management System during replacement to provide a continuous source of jacking gas to protect the journal and thrust bearing.

The electronic monitoring and control assembly is divided into three separate modules (Voltage Regulator/Exciter, Speed Control, and Signal Conditioning) which are independently packaged. The speed control portion is further divided into three LRUs, one to sense each phase of the 1200 Hz, 120 V, 12.5 kWe alternator output and apply or remove parasitic loading to maintain constant frequency under varying load and alternator output conditions. Each control circuit loads all three phases simultaneously. Each replaceable unit provides a total of six kilowatts of parasitic load so any one control circuit can be in the OFF position without affecting overall system performance.

The retractable shield is used for nuclear radiation reduction and is capable of being retracted to allow a thermal radiation path from the heat source to the inside of the spacecraft for emergency cooling. At launch, the heat shield contains 5 inches of LiH to meet the dose criteria for the first 2 1/2 years. Additional shielding of 3 inches of LiH and 0.2 inch of depleted U238 is required to meet the dose criteria for the period from 2 1/2 to 10 years.

Section 4

OCS CHECKOUT STRATEGIES

4.1 SUBSYSTEM CHECKOUT STRATEGY

Before further requirements analysis, it is necessary to develop a checkout strategy for all Space Station subsystems to meet checkout objectives, which can be summarized as follows:

- To increase crew and equipment safety by providing an immediate indication of out-of-tolerance conditions
- To improve system availability and long-life subsystems assurancy by expediting maintenance tasks and increasing the probability that systems will function when needed
- To provide flexibility to accommodate changes and growth in both hardware and software
- To minimize development and operational risks

Specific mission or vehicle-related objectives which can be imposed upon subsystem level equipment and subsystem responsibilities include the following:

- OCS should be largely autonomous of ground control.
- Crew participation in routine checkout functions should be minimized.
- The design should be modular in both hardware and software to accommodate growth and changes .
- OCS should be integrated with, or have design commonality with, other onboard hardware or software .
- The OCS should use a standard hardware interface with equipment under test to facilitate the transfer of data and to make the system responsive to changes.
- Failures should be isolated to an LRU such that the faulty unit can be quickly removed and replaced with an operational unit.

- A Caution and Warning System should be provided to facilitate crew warning and automatic "safing" where required.

- Provisions must be included to select and transmit any part or all of the OCS test data points to the ground.

To attain these objectives via the use of an Onboard Checkout System which is integrated with the Data Management System, checkout strategies have been developed which are tailored to each Space Station subsystem.

Special emphasis has been applied to a strategy for checkout of redundant elements peculiar to each subsystem. The degree to which each of these functions is integrated into the DMS is also addressed.

4.1.1 SPACE STATION SUBSYSTEMS

Each major Space Station subsystem was examined with respect to the required checkout functions. The checkout functions associated with each subsystem are identified and analyzed as to their impact on the onboard checkout task. The functions considered are those necessary to verify operational status, detect and isolate faults, and to verify proper operation following fault correction. Specific functional requirements considered include stimulus generation, sensing, signal conditioning, limit checking, trend analysis, and fault isolation.

The Electrical Power Subsystem (EPS) consists of dual Isotope/Brayton power conversion elements and a power control and distribution network. The power conversion elements include the isotope heat sources and aeroshells, heat exchangers, turbines, compressors, alternators, and Gas Management Systems. The control and distribution network consists of transformer/rectifier assemblies, voltage regulators, static sine wave and square wave inverters, batteries, battery chargers, and circuit protection and switching devices.

4.1.1.1 Checkout Functions

The EPS encompasses a wide variety of equipment including electrical, electronic, mechanical, and fluid systems. This results in a diversity of checkout requirements as identified in the following sections.

- Stimulus Generation - Stimulus generation requirements imposed by the EPS, except for control and switching purposes, are relatively few and simple. These consist of simulated current unbalance inputs required to periodically test the operation of differential protection relays, simulated reverse current inputs to periodically test reverse current sensors, and simulated phase unbalance (open phase) signals to test phase balance protection circuits. These stimuli may take the form of fixed value currents or voltages, depending upon the final design of the protection circuitry.

- Sensing - Sensing requirements imposed by the EPS are listed in Appendix I of the Task 1 Final Report. Measurement sensor and transducer requirements are generally well within current instrumentation capabilities. Sensor outputs are directly measurable as a dc voltage within specified ranges, or are converted to standard measurement voltages by appropriate signal conditioning circuitry.

  Selected sensors are implemented redundantly due to the criticality of the measurement or to the difficulty of replacing a failed unit. Critical parameters with redundant instrumentation include heat source temperature, compressor inlet temperature, compressor discharge pressure, turbine inlet temperature, bearing cavity pressures, and turbine speed. These redundant sensors provide the opportunity to perform cross correlation and calibration of measurements.

- Signal Conditioning - Signal conditioning is required for all sensor outputs which do not fall within the standard measurement capability of the Remote Data Acquisition Units. The requirements include strain gauge temperature probe conditioning networks, ac-to-dc converters, and frequency-to-dc converters. These devices perform signal conversion and scaling as necessary to provide a standard output to the Data Acquisition System.

- Limit Checking - Limit checking routines are used to verify that critical parameters such as the isotope heat source temperatures, compressor temperature and pressures, turbine temperatures and speeds, and bearing cavity pressure remain within tolerance. Limit tests are utilized within the Power Distribution System to monitor bus currents and voltages and to monitor the states of automatic circuit protection devices such as circuit breakers and phase balance protection relays.

- Trend Analysis - Opportunities to apply trend analysis techniques to the EPS are limited. Meaningful trend data may be obtained from selected temperature measurements in the isotope heat source and in certain equipment items. The latter include bearing temperatures in the rotating machinery, and heat sink temperatures in equipment such as voltage regulators and inverters. These are relatively short-term trend parameters and may provide indications of degradation or incipient failure. Longer term trend parameters include heat exchanger and radiator inlet/outlet temperatures and flow rates which may be used to identify and project efficiency degradation in these systems.

- Fault Isolation - Fault isolation is accomplished through comparison of measured operating conditions with predetermined limits and by combinatorial analysis of input/output measurements and associated performance parameters. Redundant element substitution is also used where available.

4.1.1.2 Redundant Element Checkout

Redundant elements in the EPS include critical protection and switching devices, transformer/rectifier units, voltage regulators, 400-Hz square wave inverter, 60-Hz and 400-Hz sine wave inverters, 600-Hz motor/generator, batteries, and battery chargers. These are isolatible by switching. Checkout of the redundant units is accomplished by switching them on-line periodically and verifying proper functioning under normal operating conditions. A special situation exists in the case of the 600-Hz motor/generators, as both the primary and redundant units are normally used only to provide motoring start current to the Brayton cycle 1200 Hz alternator, a function normally performed only during initial activation of the Space Station. Periodic checkout of these units therefore requires a dummy load to substitute for the alternator and permit testing to be performed without interrupting alternator operation.

The inverters also present a special case. These units are not designed for parallel operation. A redundant off-line unit cannot be rotated on line without first interrupting the ac loads. To avoid this, a dummy load is provided for checkout of redundant inverters.

4.1.1.3 Integration with Data Management Subsystem

Stimulus requirements in the EPS involve primarily fixed value currents or voltages associated with testing of circuit protection devices. These devices are distributed throughout the Space Station rather than being concentrated, and the devices themselves are generally relatively simple. This combination of conditions favors external rather than built-in stimulus generation. A requirement is therefore imposed on the DMS to generate these stimuli and to control their application to the appropriate EPS test points.

Measurement sensors, transducers, and signal conditioning for the EPS are provided as an integral part of that subsystem. The signal interface between the EPS and the DMS is in the form of a DC voltage for each measurement. The voltage levels are in the ranges of 0.20 mV, 0-5 V, and 0-28 V.

4.2 INTEGRATED CHECKOUT STRATEGY

This analysis identifies the integrated checkout functions associated with Space Station subsystems during the manned orbital phase of the mission. These functions are depicted in Figure 4-1 and are those required to ensure overall availability of the Space Station. Characteristic of integrated testing is the fact that the test involves subsystem interfaces, and, therefore, test objectives are associated with more than one subsystem.

4.2.1 INTEGRATED STRATEGY

Six checkout functions have been identified:

- Caution and warning
- Fault detection
- Trend analysis
- Operational status
- Periodic checkout
- Fault isolation

These functions represent a checkout strategy of continuous monitoring and periodic testing with eventual fault isolation to a line replaceable unit (LRU). Under this aspect the functions are grouped as -

CONTINUOUS MONITORING	PERIODIC TESTING	FAULT ISOLATION
• Caution and warning	• Automatic tests	• Localize to SS
• Fault detection	• Operational Verification	• Isolate to RLU
• Trend analysis		
• Operational status		

General characteristics of these groups are defined below:

4.2.1.1 Continuous Monitoring

Continuous monitoring is not a test per se. It is a concept of continuously sampling and evaluating key subsystem parameters for in/out-of-tolerance conditions. This evaluation does not necessarily confirm that the subsystems have failed or are operating properly. The evaluation is only indicative of the general status of the subsystems. For example, a condition exists where the integrated subsystems are indicating in-limit conditions, but during the next series of attitude control commands, an error in Space Station position is sensed and displayed. Since

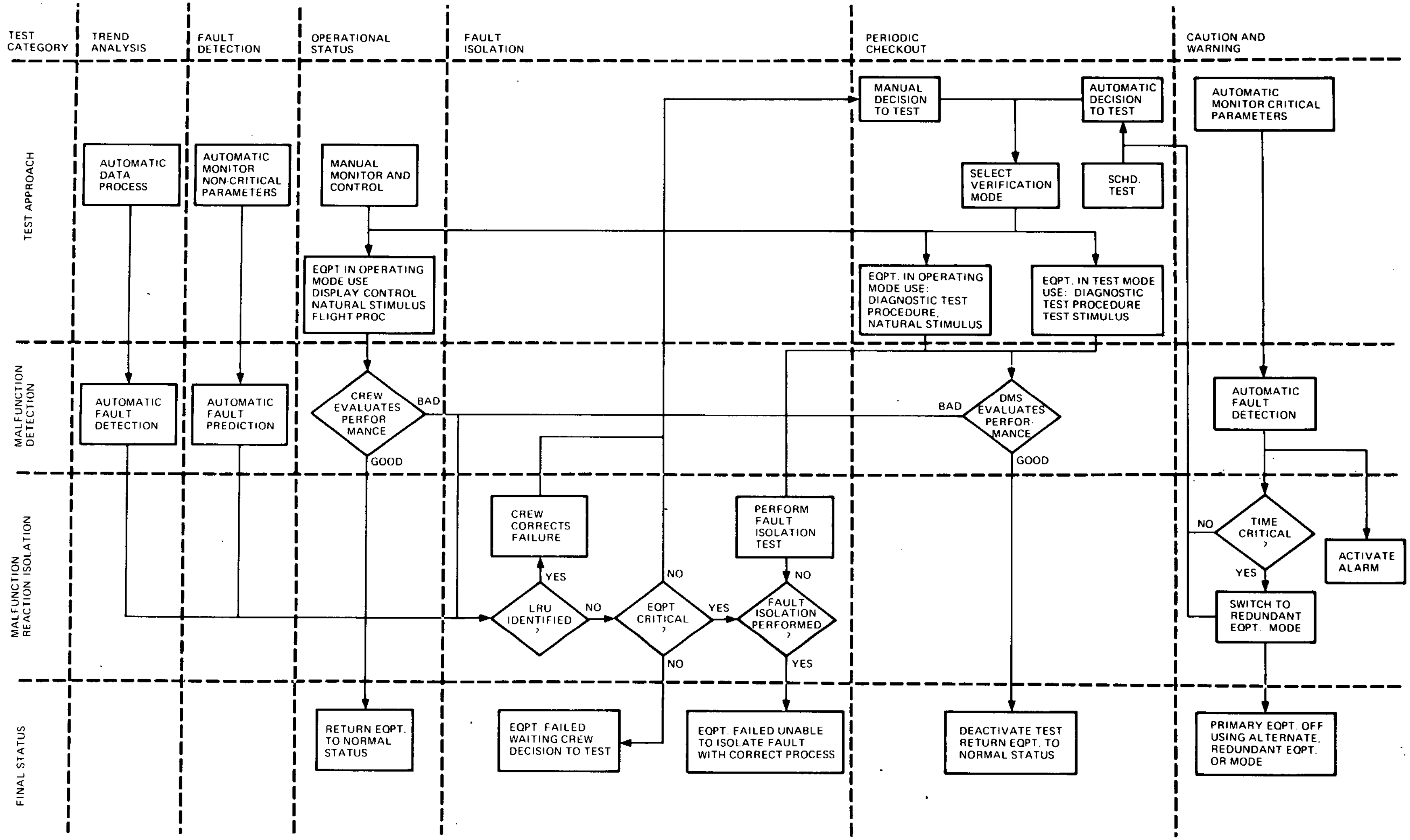


Figure 4-1. Integrated Checkout Functional Flow

three subsystems, DMS, GN&C, and P/RCS, are involved in generating and controlling the Space Station attitude, a "positional error" malfunction is not directly related to a subsystem malfunction. The malfunction indication is only indicative of an out-of-tolerance condition of an integrated function. Final resolution of the problem to a subsystem and eventually to LRU will require diagnostic test-procedures that are separate from the continuous monitoring function.

There are situations in which the parameters being monitored are intended to be directly indicative of the condition of a subsystem or an LRU. Examples of these include tank pressures, bearing temperatures, and power source voltages. However, even in these simpler cases when a malfunction is detected, an integrated evaluation will be performed to ascertain that external control functions, transducers, signal conditioning, and the DMS functions of data acquisition, transmission, and computation are performing properly. This evaluation will result in either a substantiation of the malfunction or identification of a problem external to the parameter being monitored.

Figure 4-1 shows the logic associated with each function in the continuous monitoring group, as well as the integrated relationships between these and the total checkout functions. The caution/warning and fault detection functions are alike in their automatic test and malfunction detection approaches, but are different in terms of parameter criticality and malfunction reaction. The caution/warning function monitors parameters that are indicative of conditions critical to crew or equipment safety. Parameters not meeting this criticality criteria are handled as fault detection functions. Figure 4-1 shows that in the event of a critical malfunction, automatic action is initiated to warn the crew and sequence the subsystems to a safe condition. Before this automatic action is taken, the subsystems must be evaluated to ascertain that the failure indication is not a false alarm and that the corrective action can be implemented. After the action is taken, the subsystems must be evaluated to determine that proper crew safety conditions exist. Since automatic failure detection and switching can be integral to subsystem design (self-contained correction) and subsystems can be controlled by the operational software or manual controls, it is imperative that the status of these events be maintained and that the fault detection and correction software be interfaced with the prime controlling software. For malfunctions that are not critical, the crew is notified of their occurrence, but any subsequent action is initiated manually.

The next continuous monitoring function, trend analysis, automatically acquires data and analyzes the historical pattern to determine signal drift and the need for unscheduled calibration. It also predicts faults and indicates the need ~~for diagnostic and fault isolation activities. An example of a parameter in this~~ category is the partial pressure of nitrogen. Nitrogen is used to establish the proper total pressure of the Space Station. Since it is an inert gas, the only makeup requirements are those demanded by leakage or airlock operation. The actual nitrogen flow rate is measured, and calculations are performed which make allowances for normal leakage and operational use. When these calculations indicate a trend toward more than anticipated use, the crew is automatically notified and testing is initiated to isolate the problem to the gas storage and control equipment or to an excessive leak path. The historical data is not only useful in predicting conditions but is also useful in providing trouble-shooting clues. The data might reveal, for example, that the makeup rate increased significantly after the use of an airlock. This could lead directly to verifying excessive seal leakage.

The final continuous monitor function is in operational status. This function is performed by the crew and is nonautomatic with the exception of the DMS computer programs associated with normal Space Station operational control and display functions. The concept of continuous monitoring recognized and takes advantage of the crew's presence and judgment in evaluating Space Station performance. In many instances the crew can discern between acceptable and unacceptable performance, and they can clearly recognize physically-damaged equipment or abnormal conditions.

4.2.1.2 Periodic Testing

As opposed to continuous monitoring, periodic testing is a detailed evaluation of how well the Space Station subsystems are performing. Figure 4-1 shows that periodic testing is not accomplished by any one technique. Rather, a combination of operational and automatic test approaches is employed. The actual operational use of equipment is often the best check of the performance of that equipment. Operation of Space Station equipment and use of the normal operating controls and displays will be used in detecting faults and degradation in the subsystems. This mode of testing is primarily limited to that equipment whose performance characteristics are easily discernible, such as for motors, lighting circuits, and alarm functions.

Automatic testing is performed in two basic modes:

- With the subsystems in an operating mode, the DMS executes a diagnostic test procedure which verifies that integrated Space Station functions are being properly performed under normal interface conditions in response to natural or designed stimulation. This mode of testing allows the evaluation of Space Station performance without interrupting mission operations.

- For those situations where the integrated performance or interface compatibility between subsystems cannot be determined without known references or control conditions, the DMS will execute a diagnostic procedure in a test mode. In this mode, control, reference, or bias signals will be switched in or superimposed on the subsystems to allow an exact determination of their performance or localization of problem between the interfaces. Since the test mode may temporarily inhibit normal operations, the DMS must interleave the test and operational software to maintain the Space Station in a known and safe configuration.

The scheduled automatic tests are performed to verify availability or proper configuration of "on-line" subsystems, redundant equipment, and alternate modes.

- Periodic Verification of "On-Line" Subsystems - The first checkout requirement is a periodic verification that on-line subsystems are operating within acceptable performance margins. The acceptable criteria for this evaluation is based on subsystem parameter limits and characteristics exhibited during Space Station factory acceptance or pre-flight testing. The rejection criteria and subsequent decision to repair or reconfigure subsystems is based on the criticality of the failure mode. If the subsystems appear to be operating properly, but the test clearly indicates an out-of-tolerance condition, then one of the following alternatives must be implemented:

  - If the failure mode is critical, the crew normally takes immediate action to isolate and clear the problem.

  - If the failure mode is not critical, the crew can take immediate action, schedule the work at a later time, or wait until the condition degrades to an unacceptable level.

- Redundant Equipment Verification - A second checkout requirement is verifying that standby, off-line, or redundant equipment and associated control and switching mechanisms are operable. The acceptable/rejection criteria for these evaluations is identical to those for normally operating equipment. A primary distinction of this function is that equipment may have known failures from previous usage or tests. This situation occurs when the crew has knowledge of a failure but has not elected to perform the necessary corrective action. The checkout function then becomes one of equipment status accounting and maintenance/repair scheduling. The status information is interlocked with mission procedures and software to preclude activation of failed units while they are being repaired or until proper operation following repair is verified.

- Alternate Mode Verification - The third checkout function is verifying the availability of alternate modes of operation. This function is essentially a confidence check of the compatibility of subsystems' interaction and performance during and after a change in the operating mode. To some extent this function overlaps with redundant equipment verification, but is broader in scope in that it verifies other system-operating characteristics. For example, some modes will involve manual override or control of automatic functions or automatic power-down sequences.

4.2.1.3 Fault Isolation

Fault isolation to an LRU is a Space Station goal. As shown in Figure 4-1, fault isolation testing is initiated when malfunction indications cannot be directly related to a failed LRU. The integrated test functions associated with fault isolation are localizing a malfunction to a subsystem or to an explicit interface between two subsystems and identifying the subroutine test necessary for LRU isolation. In structuring this relationship between integrated subsystem tests for fault localization and subroutine tests for fault isolation, the DMS, in conjunction with the test procedure documentation, must establish an effective man-machine interface so that in the event of an unsolved malfunction the crew will be able to help evaluate the condition and determine other test sequences necessary to isolate the problem. To accomplish this requirement, the DMS must be capable of displaying test parameters and instructions in engineering units and language and be capable of referencing these outputs to applicable documentation or programs that correlate test results to corrective action required by the crew.

Section 5

ONBOARD CHECKOUT TEST DEFINITIONS

5.1 SUBSYSTEM TEST DEFINITIONS

The on-orbit tests required to insure the availability of the Space Station subsystems are defined herein. Also delineated are the measurement and stimulus parameters required to perform these tests. Two discrete levels of testing are defined, i.e., continuous status monitoring tests for fault detection of critical and noncritical parameters, and subsystem fault isolation tests for localization of faults to a specific Line Replaceable Unit. In addition to these two levels, tests are defined for periodic checkout and calibration of certain units, and parameters requiring analysis of trends are defined.

Due to the software module approach to DMS checkout, it was deemed necessary to estimate the CPU time and memory required to implement these modules along with an assessment of the services required from an Executive Software System to control the checkout.

These test descriptions, measurement, and stimulus information provided for each subsystem, and the software sizing information provided for the Data Management System provide the data required to estimate the checkout impact on the DMS software and hardware. Table 5-1 is a summary of the measurement and stimulus requirements for the Space Station.

The baseline Electrical Power Subsystem (EPS) consists of dual Isotope/Brayton power conversion systems and a transmission, conditioning, and distribution system.

5.1.1 POWER CONVERSION SYSTEM

The Isotope/Brayton System (IBS) produces the electrical power for the Space Station by converting thermal energy from plutonium isotope heat sources to electrical energy through Brayton cycle turbine-driven alternators.

The IBS consists of the heat source assemblies, heat exchangers, rotating power conversion units, Gas Management System, and voltage-regulator/speed control assemblies. The system also includes an atmosphere reentry and recovery system (IRV) for emergency jettison and return of the heat sources.

Table 5-1. Measurement/Stimulus Summary

SUBSYSTEM	STIMULUS					RESPONSE			STATUS MONITORING								
	Analog	Bilevel	Digital	Pulse	RF	Analog	Bilevel	Digital	Total	Non-Critical	Caution	Warning	Periodic Checkout	Cali-bration	Trend	Fault Isola-tion	Remarks
Guidance, Navigation and Control	20	146	62	6		127	161	70	592	130	16		516	74	74	592	
Propulsion - Low Thrust		134				120	124		378	152	14		378	48	8	378	
Propulsion - High Thrust		126/62				287/117	123/63		536/242	80/28	33/15	14/10	536/242	259/111	117/43	482/222	Art-g/Zero-g periods
Environmental Control/ Life Support	34	111				691	280		1116	139	205	32	1116		135	1116	172 Caution/Warning Signals are for IVA/EVA
RF Communications	37	206	36		77	131	286	28	801	58			576	24	93	801	
Structures	15/16	21/19				60/53	75/66		174/154	7			123/104			174/154	
Electrical Power - TCD	52	1952				292	1292	20(1)	7608	1404	20		724		134	3608	(1) Twelve of these take pulse form
Electrical Power - Solar Array/Battery		1916				4044	928		6780	3704	12		2184		332	6788	
Data Management			53			33	188	83	357	357			62	62	62	357	
Total	151/169	4512/ 4446	151	6	77	5785/ 5628	3457/ 3388	201	14,350/ 14,035	6031/ 5979	300/282	46/42	5110/ 5902	467/ 319	935/ 861	14,266/ 14,016	

Appendix I-7 of the Task 1 Final Report contains a listing of the measurements and stimuli associated with the IBS.

Operation of the IBS is in a closed-loop automatic mode and is controlled by the Data Management System (DMS).

To provide heat source control, the compressor inlet temperature, turbine inlet temperature, heat source capsule hot spot temperature, and BeO hot spot temperature are processed by the heat source control logic. Position indicators tell when the heat source is in the "operating" mode and when it is extended and radiating into space in the "emergency cooling" mode.

The power conversion Brayton gas loop is controlled by the turbine inlet temperature, the compressor inlet temperature, the bearing cavity pressure, and the compressor outlet pressure.

In addition to the gas loop instrumentation, there are several electrical parameters included with the Power Conversion System to provide fault detection and control for the alternator. These are alternator output, load bus, series and shunt field currents, alternator output voltage, and frequencies. The voltages, currents, and frequencies together with voltage regulators/exciter and speed control circuitry provide the signals necessary to maintain specified speed and voltage regulation. They also provide the signals vital to normal startup and shutdown as well as emergency control in case of critical level out-of-tolerance voltages, currents, and speeds.

The Gas Management System contains pressure and temperature transducers for monitoring the status of the reserve supply of the Xe-He gas for the power conversion loop. It also includes several valves to provide a controlled gas supply to the thrust bearings, journal bearings, and for maintenance of the loop gas inventory. Auxiliary contacts on each valve act as positive position indicators to show the status of the valves.

The IRV is utilized only for emergency disposal of the heat source. It consists of an ejection mechanism, passive stabilization and control system, ballute type descent system, and recovery aids such as radio beacon and flashing light.

5.1.1.1 Status Monitoring

Status monitoring is utilized on selected performance parameters to detect system faults. Acceptance or rejection of status measurements is based upon comparison of the measured values against predetermined limits and/or against parallel redundant parameters.

The majority of the status monitoring parameters are safety critical and are treated as caution and/or warning parameters. Detection of an out-of-limit condition in one of these measurements results in activation of the crew alarm and also in the initiation of automatic fault isolation and safing procedures. Certain parameters are identified in both the caution and the warning category. These involve two-level limit checking.

5.1.1.2 Trend Analysis

Trend analyses are applicable to several of the IBS functions. In particular, analysis of temperatures and pressures in the Brayton loop and heat rejection loops is useful in ascertaining the efficiency of the system and spotting degradation in performance. The trends of critical heat source temperatures are of interest from a safety standpoint.

5.1.1.3 Periodic Checkout

Periodic tests are required to supplement the continuous status monitoring in order to make a quantitative evaluation of system operating characteristics and to verify the operation of standby or inactive systems. Items in the latter category include the drive mechanisms for extending the heat sources to their emergency cooling positions and the IRV Systems. The test sequence is not critical but normally begins with verification of the DMS control interfaces, followed by checking of the IRV Systems and heat source extension mechanisms. It should be noted that functional testing of the extension systems requires short-term interruption of power generation in the unit being tested. Power distribution and consumption during this period must be managed accordingly, and proper operation must be reverified upon completion of the test.

5.1.1.4 Fault Isolation

The IRV heat source and Brayton power conversion loop are major subsystems that are line replaceable units. The Gas Management and Heat Rejection Systems are line replaceable at the component level. Electrical control components such as the voltage regulator exciter and speed control are line replaceable as individual units. Integration of the radiator cooling flow tubes into the vehicle structure precludes inclusion of the Heat Rejection System as a line replaceable unit. Instead, the components are either line replaceable or have built-in redundancy. The Heat Rejection System itself is a redundant element of the Power System so that the Power System electrical production does not have to be disturbed during the replacement of components. The pump motor has instrumentation to isolate pump failures (pump pressure out and flow rates) from power failure (pump current and voltage). Deterioration of the pump motor can be detected from trend analysis of the power drawn by the unit and the deterioration can be segregated from deterioration of the fluid cooling loop or coolant by comparing the change in power drawn (motor current) with the pump head (pump outlet pressure). Changes in individual flow rates, temperature rise across cold plates, and hot spot temperatures can be used to isolate cooling (cold plate) failures from failures in the components they are designed to cool. Radiator outlet temperature is an important parameter for judging the condition of the fin surface coating of the radiator. At any instance, only one heat rejection loop for each Power Conversion System is operating and only one of the two pumps is in operation so that only one set of transducer signals are needed to provide data. The hot spot temperatures are critical parameters, however, and the triple redundancy is required to isolate instrumentation faults from operating system faults to prevent false caution signals.

A typical fault isolation flow is illustrated in Figure 5-1. Here a fault in the heat rejection pump gives the first indication of a fault by setting off the caution alarm for the isotope heat source capsule temperature. The chart demonstrates that even though the fault occurred in a component far removed from the parameter that gave the indication, adequate instrumentation is available to isolate the fault at the faulted component. In actual practice, more than one fault alarm may occur (such as capsule temperature and pump hot spot temperature, or capsule temperature and compressor outlet temperature) which would lead directly to isolating the fault.

5.1.2 TRANSMISSION, CONDITIONING, AND DISTRIBUTION

This section discusses the monitoring and control requirements for the Transmission, Conditioning and Distribution (TCD) portion of the EPS. Appendix I-8 provides a TCD measurement/stimulus list which identifies the specific parameters, stimuli, and response functions required to check the system and to determine its operational status.

The TCS System requires a minimum of crew supervision. Operational parameters consist of alternator feeder current readouts, battery status, and principal primary and secondary bus voltages. The feeder current readouts, together with alternator output power displays establish the degree of load balance between the two Brayton PCS units. A small amount of unbalance is inherent in the system. Crew action is required only if the normal range is exceeded (as detected by the Power Management Assembly), or if high experiment activity requiring maximum possible power from the Brayton machines is imminent. Crew response under these conditions is to shift load from one machine to the other by selective switching of loads.

Battery status displays and readouts of selected bus voltages provide additional information for evaluating system performance and capability for accepting additional load. The ability to call up the status of any other system element, as may be deemed necessary for evaluation of a particular operational condition, provides the flexibility required to ensure adequate status assessments at any given time.

All circuit breakers and contactors for power transmission lines, source and distributor buses, and power conditioning equipment can be remotely controlled. Many are controlled by signals from automatic protection equipment such as differential or reverse current relays. Remote control is also required to provide for either manual or programmed reconfiguration of the TCD System following automatic fault-clearing operations, as well as for facilitating reconfiguration to match changing load or other operational conditions. Additional controls are provided to support checkout functions.

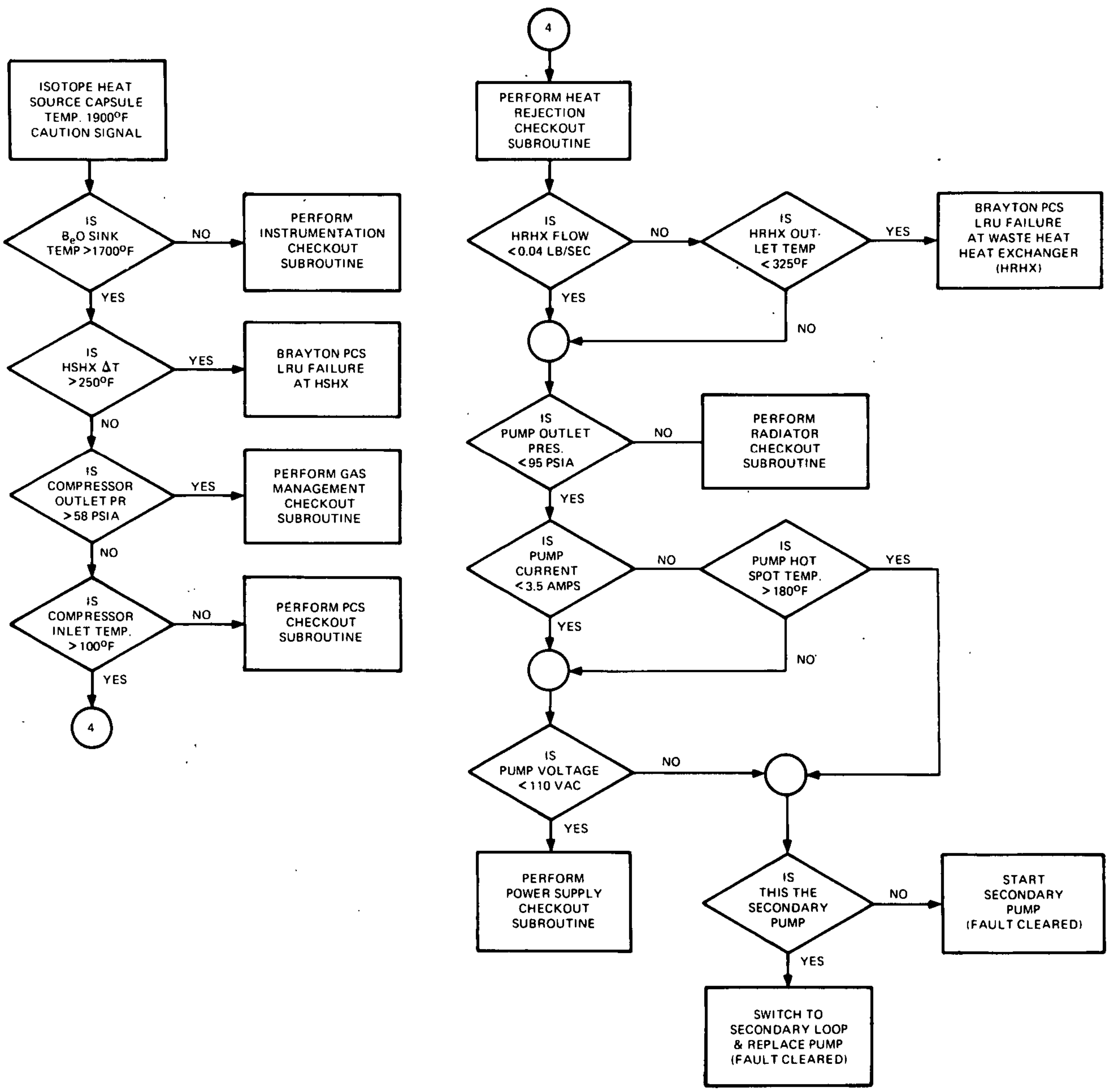


Figure 5-1. Typical LRU Malfunction Isolation Flow Chart

It is important to note at this point that no capability is shown for remote control of individual circuit breakers in the distribution circuits to the loads. It is assumed for the purpose of this study that all switching of loads is accomplished in the load systems themselves rather than by opening and closing circuit breakers in the power lines to individual loads. Final definition of load switching control design is yet to be developed.

5.1.2.1 Status Monitoring

Continuous monitoring is required to detect out-of-tolerance conditions for parameters such as alternator load-sharing, principal bus voltages, and equipment temperatures. Continuous monitoring is also required to detect abnormal events. These include relay trips, circuit breaker and contactor trips, and power conditioner overload (current limiting signal).

Alternator feeder currents and most bus voltages are sampled at the rate of six per minute. Feeder current values should stay fairly constant during normal operation, but as previously mentioned, some unbalance is inherent. A sampling rate of six per minute for bus voltages should eliminate the effects of voltage transients (assuming a fault signal is generated only if an out-of-tolerance condition is sensed in two consecutive samples), while still providing a reasonable response time for follow-on corrective action. The higher sampling rate of once per second for 28 Vdc and 400 Hz load bus voltages assures minimum delay in detecting out-of-tolerance voltages at the principal load interfaces. For this higher rate, abnormal voltage should be sensed in a minimum of five consecutive samples before a fault signal is generated.

Equipment temperatures are sampled at a rate of four per hour. Considering thermal lags inherent in the equipment being monitored, this rate should be adequate for all but catastrophic failures.

Relay trips are nominally monitored at a one-sample-per-minute rate. Circuit breaker and contactor trips are sampled at a rate of two per minute. This allows a margin for contact opening time before the next sample is taken. If the next sample does not show a contactor trip, it is presumed the contactor will not operate to clear the fault and alternate corrective action is immediately taken. An exception to the nominal sampling rates is shown for the alternator feeder/source bus differential relays. The rate here is one sample per second. This is because operation of these relays results in tripping the associated alternator circuit breaker, with a consequent loss of one-half the station primary power. The sampling rate for the alternator circuit breaker is five per second, also much higher than nominal. These relatively high rates are required to minimize system and load disturbances in switching to a backup mode of operation.

A sampling rate of two per minute is chosen for detection of power conditioning equipment operating in a current-limited overload mode. Again, this allows a margin for transient overloads.

No life-critical functions have been identified for the TCD System. An unscheduled opening of the alternator feeder circuit breaker, however, results in loss of one-half of the primary power source and is therefore listed as a caution function. Loss of 260 Vdc bus voltage is also listed since this results in interruption of all 400 Hz power. Loss of 400 Hz square wave bus voltage and loss of 400 Hz sine wave bus voltage are included since they result in interruption of all 400 Hz square wave and sine wave power, respectively.

5.1.2.2 Periodic Checkout

Periodic checkouts will be performed at intervals ranging from once per week to once each six months depending on equipment or parameters to be checked.

The principal tests required to ensure TCD System performance, integrity, and availability are listed in Table 5-2. In addition to these tests, checks of selective switch positions, interlocks, system load distribution, and availability of load bank equipment are required. Tests for relay, circuit breaker, and contactor operations can generally be accomplished on line during periods of relatively low-scheduled experiment activity; system switching effects will be minimal. No major shock producing tests, such as power line faults or fault clearing, are planned.

Complexity of checkout varies from simple readouts of parameters, such as voltage or temperature, to injection of test currents into current transformer loop circuits to simulate fault conditions seen by protection relays. An example of a procedure which typifies the range of parameter testing and also illustrates the handling of redundant units is given in Table 5-3 for the high voltage rectifier-regulators.

5.1.2.3 Calibration

No requirements for calibration are listed. A limited amount of calibration may be required for certain relay installations. This has not been analyzed at this time.

5.1.2.4 Trend Analysis

A limited amount of trend analysis is necessary for TCD parameters. These are identified in Appendix I-7 of the Task 1 Final Report.

Table 5-2. Transmission Conditioning and Distribution System Periodic Tests (Isotope/Brayton)

Test	Rationale
Protective Relay Operation	To verify proper operation of protective devices
Circuit Breaker and Contactor Operation	To determine remote operability of breakers and contactors
Standby Redundant Equipment Operation	To verify operational capability of standby units
Battery Charger Mode Switching	To determine charger response to control inputs
Alternator Load Sharing	To determine whether load balance is within allowable tolerances
Regulated Transformer-Rectifier Load Sharing	To determine whether load balance is within allowable tolerances
Power Conditioning Equipment Parameters	To determine nominal performance capability and degradation, if any, with respect to like units
Bus Voltages	To assess general health of TCD system
Battery Monitor Voltage and Temperature	To determine battery status

5.1.2.5 Fault Isolation

Control signals for opening and closing remotely operable circuit breakers, contactors, and switches are required for fault isolation. These signals are operated internal to the TCD System (e.g., differential protection sensing and relay output) to provide coordinated automatic fault clearing, and external to the system for checkout purposes. A typical fault isolation flow diagram is given in Figure 5-2.

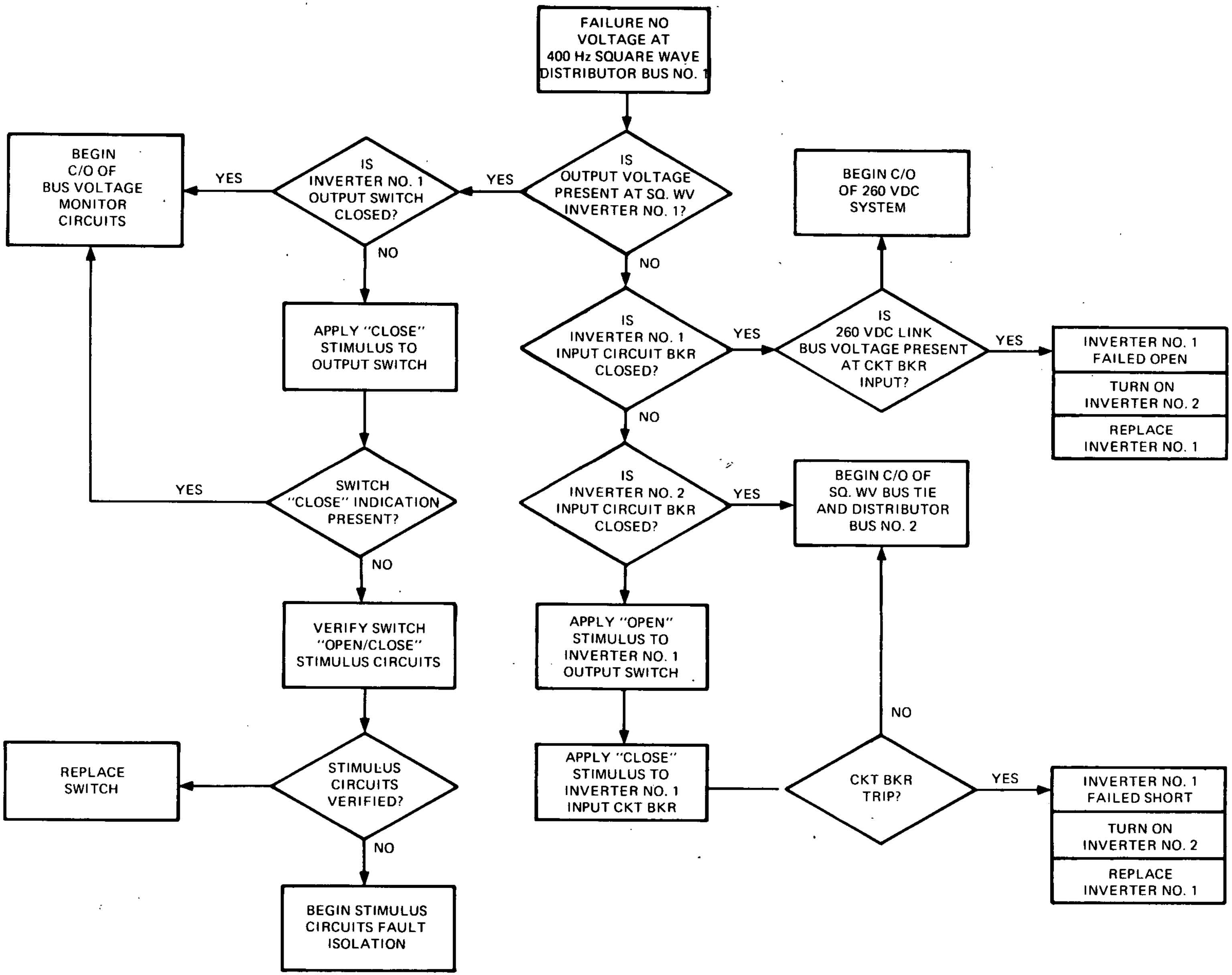


Figure 5-2. Typical Fault Isolation Flow Diagram

Table 5-3. Periodic Checkout High Voltage Rectifier-Regulators

1. Apply primary power to one off-line redundant unit.
2. Monitor open-circuit output voltage level.
3. Apply overload test current to secondary of current limiting sensing circuit and monitor for current limiting mode alarm.
4. Remove test current and reset current limiting mode alarm circuit.
5. Repeat steps 1 - 4 with second off-line redundant unit.
6. Connect first off-line unit to 260 Vdc bus and verify that input current, output current, and output voltage are within specified limits.
7. Repeat step 6 with second off-line unit.
8. Verify that the two units share load within specified limits.
9. Disconnect the two previously on-line units and assign them to the standby redundant mode.
10. Reverify load sharing between the two on-line units.
11. Continue operation with the new unit assignments until the next checkout period or until reconfiguration is required for other operational reasons.

5.2 INTEGRATED TEST DEFINITION

The task of ensuring overall Space Station availability is primarily dependent upon the proper structuring of individual subsystem tests. The ability to test the subsystems independent of other subsystems is directly related to the number and types of interfaces. As shown in Figure 5-3, the DMS and Electrical Power Subsystems (EPS) interface with every other Space Station subsystem. In addition, the EC/LS Subsystem provides cooling to most of the electronic packages.

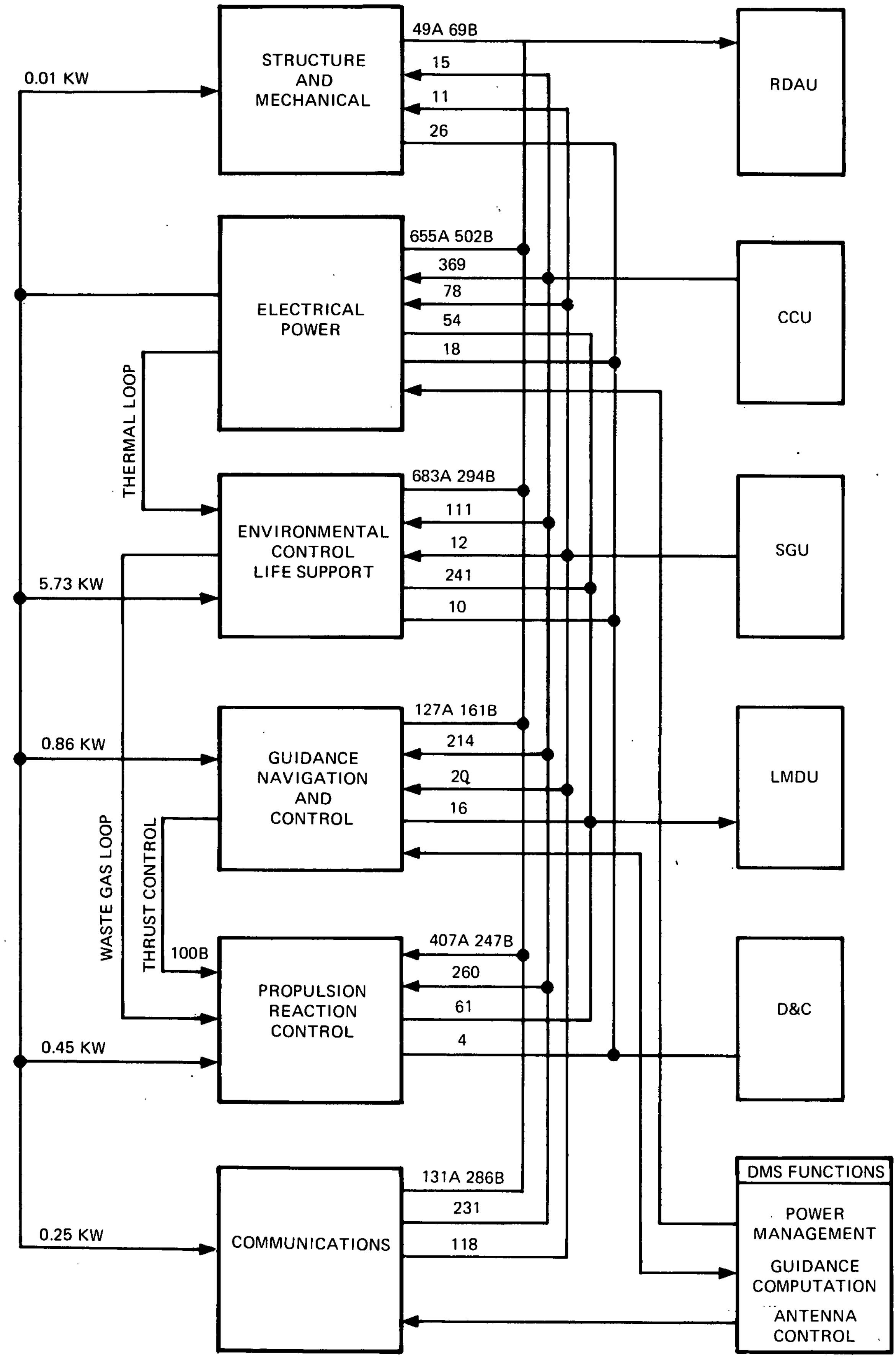


Figure 5-3. Subsystem Interfaces

This situation demands that in constructing the test for a subsystem these interfaces be taken into account so that erroneous or ambiguous test results will not be obtained. In other words, before detailed subsystem fault isolation tests are initiated, a higher level of testing should be performed to verify that all interfaces and Space Station conditions that influence the subsystem are proper. Properly designed, these higher-level tests will (1) indicate what Space Station conditions must be verified, maintained, or changed; (2) localize the malfunction to a single subsystem; and (3) identify the subroutine test necessary for fault isolation.

Since the DMS interfaces with all of the Space Station subsystems and is used as the OCS, it would appear that all of the tests would be integrated. However, this is not a proper interpretation. When the DMS is used to verify the performance of another subsystem, it must first establish itself as a test standard against which the subsystem parameters are compared. Subsequent to this verification, the test is dedicated to the evaluation of the subsystem. This test would be considered as an independent test since the objective of the test was to verify the subsystem and not the DMS. For a test to be considered as an integrated test it must meet one or more of the following conditions:

- Test objectives associated with more than one subsystem
- Test involves subsystem interfaces
- Test requires proper operation of other subsystems

In several cases, the DMS must simultaneously perform the dual role of OCS and functional elements. As an example, the DMS has a functional interface with the GN&C and Prop Subsystems for the computation of guidance equations and the execution of commands to the control actuators. When this functional closed loop is being tested, the DMS must, in addition to performing its normal functions, execute the test routine. For this type of integrated test there must be an intrinsic relationship between the operational and test software. This relationship must be carefully considered in structuring the integrated tests since unstable or intermittent performance may be detected only in the exact operating mode under closed-loop conditions. The number of integrated tests is not extensive due to the approach of minimizing the different types of interfaces between Space Station subsystems. For example, interfaces between the DMS and other subsystems are largely standardized. As a result, relatively common tests can be designed for verification of the multitude of DMS subsystem interfaces or for localization of a fault to one side of a DMS subsystem interface. All special integrated tests that have been identified are discussed in the following paragraphs.

5.2.1 DMS/EPS

The DMS has a power management interface with the Electrical Power Subsystem. This function primarily includes start-up, control and shutdown of the power conversion equipment, and the control and reconfiguring of the power profile through the distribution buses. Fault isolation is performed by a DMS self-check that verifies proper generation and transmission of control functions to the interface.

The startup, control, and shutdown of the power conversion equipment by the DMS is another example of the integral relationship that must exist between the operational and test software. For example, in starting the Isotope/Brayton System the automatic operational procedure must contain exact instructions for a normal start and an additional set of instructions for aborting or safing an abnormal start. To know the starting sequence (operational software) is not proceeding as planned implies a knowledge of what is wrong (test software). Based upon this knowledge the DMS can execute the appropriate operational controls and identify the malfunctioning element.

5.2.2 EC/LS - EPS ISOTOPE/BRAYTON INTERFACE

The Environmental Control/Life Support (EC/LS) Subsystem interfaces with the EPS Isotope/Brayton System for removal of waste heat via a fluid heat exchanger installed in the Brayton Power Conversion System. It is planned that flow rate, temperature, and pressure parameters be continuously monitored on both sides of the interface as part of normal EPS and EC/LS Subsystem checks.

5.2.3 EPS - SUBSYSTEM INTERFACE

The Electrical Power Subsystem (EPS) supplies power to all assemblies of other subsystems requiring electrical power. Interfaces between the EPS Transmission, Conditioning, and Distribution (TCD) System and other subsystem assemblies are standardized throughout the Space Station. In addition, the tests and associated measurement/stimulus requirements defined for the EPS have indicated that a comprehensive capability exists for checking TCD outputs. Fault localization between TCD assemblies and elements of other subsystems can therefore be accomplished by EPS Subsystem-oriented tests.

Section 6

SOFTWARE

6.1 GENERAL CONSIDERATIONS

The recommended software checkout startegy involves a sequence of detecting faults, isolating faults to a failing LRU or LRUs, and reconfiguring the system to continue operation while the failures are being repaired.

This recommendation was developed by evaluating each subsystem with respect to the three general requirements of fault detection, fault isolation, and reconfiguration.

Fault detection incorporates both the recognition of failure occurrence, and the prediction of when a failure can be expected to occur. The Remote Data Acquisition Units (RDAUs) continually check selected test point measurements against upper and lower limits, and notify the executive on an exception basis when a limit is exceeded. This approach avoids occupying the central multi-processor with the low-information task of verifying that measurements are within limits.

Trend analysis is a fault detection technique recommended for predicting the time frame during which a failure can be anticipated. Data is acquired on a basis of time or utilization, and compared with previous history to determine if a "trend" toward degraded performance or impending failure can be detected.

Another checkout requirement evaluated for each subsystem is periodic testing. This type of test is provided to exercise specific components at extended time intervals or prior to specific events, to assure operational integrity. In the event that a failure is detected, the periodic test will isolate to the failing Line Replaceable Unit (LRU) and accomplish recertification after a repair operation.

Calibration of specific subsystem components will be required periodically, or subsequent to a repair and/or replace operation. The techniques involved are unique to the individual component; and, in some cases, require the acquisition of operational data.

Fault isolation is required when a fault is detected. When a particular fault provides an indication that a life critical failure has occurred, the fault isolation routines are automatically initiated. If the failure does not represent an immediate danger to the vehicle occupants, the crew is notified and they will initiate the fault isolation modules at their convenience.

The basic requirements of the fault isolation function is to analyze the available information relevant to a problem, and identify the LRU which is responsible for the anomaly.

Three basic approaches to meeting this requirement were considered. These are:

- Analyze each fault as an independent problem
- Analyze each fault with a state matrix which defines the possible error states of the subsystem
- Associate each fault with a specific subsystem, and evaluate that subsystem in detail

The third approach was selected on a basis of software commonality and cost effectiveness. The complexity associated with the testing can be reduced by localization of the logic associated with the analysis of the subsystem in a unique package. The software commonality will result in reduced software development and maintenance costs, while increasing the reliability of the software.

The fault isolation software is structured modularly for compatibility with the hardware structure of the subsystem. Checkout modules evaluate the performance of a specific portion of the subsystem. A convenient division for this modular structure is at the assembly level or functional area. A program module which can determine and control the sequence in which these checkout modules are executed is also required for each subsystem.

Subsequent to fault detection, the software associated with the subsystem which is most likely to contain the error will be activated.

The subsystem software will analyze the error indication, and initiate a sequence of checkout modules to isolate the problem. If successful, the crew is notified regarding the Line Replaceable Unit (LRU) to be replaced. If an error cannot be identified, the crew is informed of the situation and has an option to execute the periodic test of the subsystem.

After a fault has been isolated, reconfiguration software restores the functional capability of the subsystem. This is most commonly accomplished by exchanging a redundant element for the failing unit, or by defining an alternate path to accomplish the required function.

The Task 2 Final Report of the basic onboard checkout techniques study provides descriptions of the software requirements, definitions and design in addition to detailed flow charts of specific checkout routines.

6.2 SPACE STATION ELECTRICAL POWER SUBSYSTEM

In this section, the technical aspects of the Isotope/Brayton (I/Br) and the Solar Array (SA) checkout programs are described. The computer program components are identified, and their functions, structure, processing, input, output, and data base requirements are discussed.

Both the Isotope/Brayton and the Solar Array configurations of the Space Station Electrical Power Subsystem (EPS) require the same general checkout program functions. Trend analysis is required for assessment of a series of measurements. Status monitoring is required to smooth the effects of transients. Fault isolation is required to locate the failed assembly and identify the LRU. Reconfiguration involves the recovery from failure. Periodic checkout exercises all modes of certain assemblies to verify proper operation. As discussed below, individual functions differ in their details depending on whether the I/Br or SA design is used.

Block diagrams of EPS in the Isotope/Brayton and Solar Array configurations are shown in Figure 6-1 and Figure 6-2, respectively.

6.2.1 SYSTEM REQUIREMENTS

Both EPS designs require that the physical laws concerning the power sources be employed in checkout. This reduces the number of test points while increasing the checkout program complexity.

Because the power supplied to other subsystems is vital to their performance, certain measurements must be made at periods of less than one seconds, which may provide the upper bound for DMS response, both from the software and the hardware standpoint.

The Electrical Power Subsystem is an essentially serial hierarchy of assemblies, compared with other subsystems of the Space Station; consequently, the modularity of EPS checkout programs is influenced by extensive interface between modules.

Transients can momentarily cause test points to exceed their limits and then return to within limits without adversely affecting the load. Therefore, the RDAU limit checking capability must be augmented by successive test point sampling at specified intervals in order to distinguish between real out-of-tolerance conditions and temporary ones.

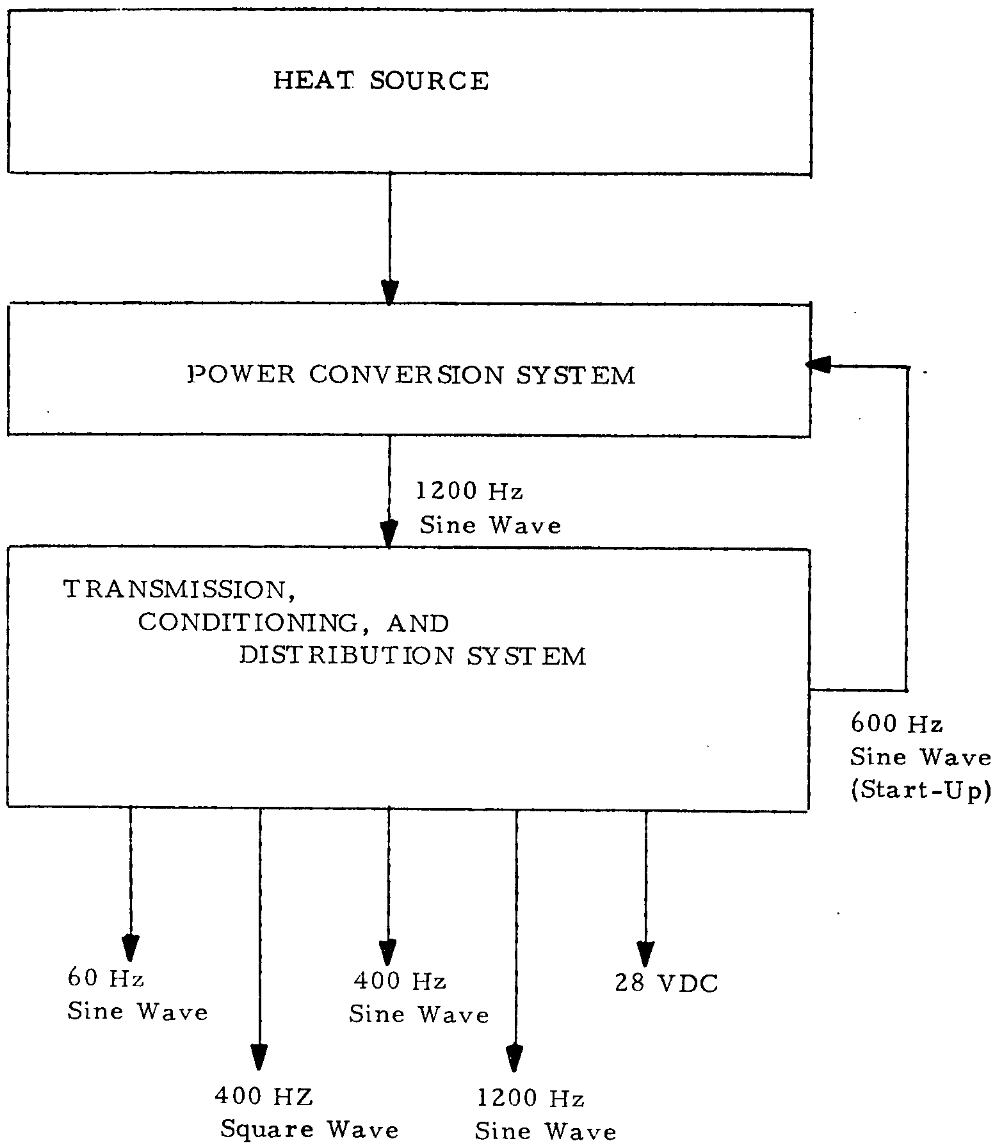


Figure 6-1. Electrical Power Subsystem Diagram, Isotope/Brayton Configuration

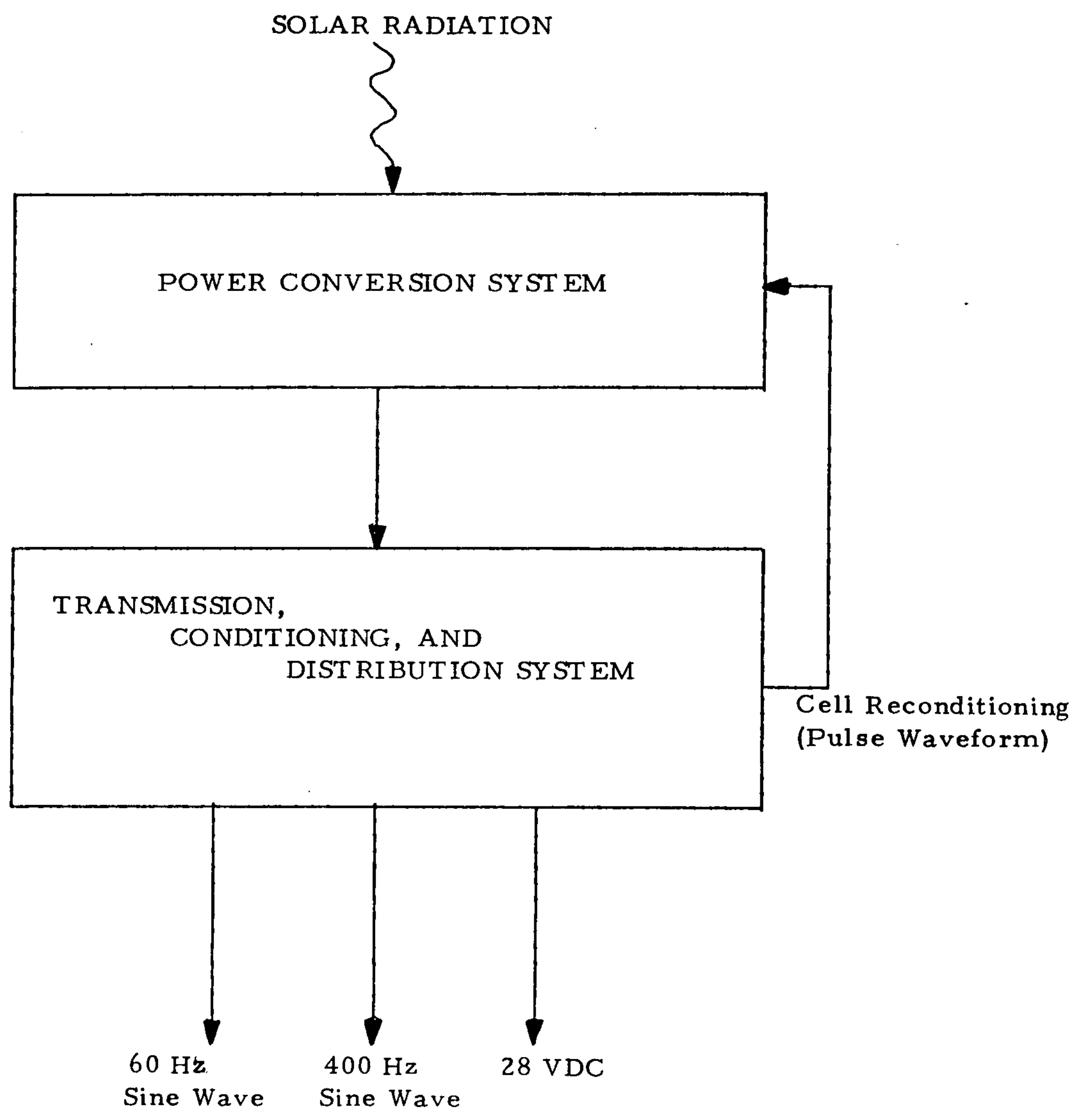


Figure 6-2. Electrical Power Subsystem Diagram, Solar Array Configuration

6.2.2 OPERATIONAL REQUIREMENTS

The EPS checkout programs are required to perform trend analysis, status monitoring, fault isolation, reconfiguration and periodic checkout.

6.2.2.1 Trend Analysis

Trend analysis is performed on selected parameters of the EPS for performance evaluation and the detection of an impending failure prior to the time when an actual out-of-limit measurement is obtained.

Input to the trend analysis function consists of control from the executive at regular intervals, status of the assembly with which the parameter is associated, and a reading of the parameter itself. The requirement to sample certain solar array parameters at a rate of once per orbit indicates a need for specifying the time at which sampling should begin, as well as the rate at which the executive will give control to the trend analysis function. The measurements previously obtained are also required as input to the trend analysis function.

Output of the trend analysis function consists of the measurement collection for storage until the next sample, displays of exceptional conditions to the crew and/or ground, and the initiation of other checkout functions such as caution and warning analysis, and fault isolation.

The trend analysis functions for the Isotope/Brayton design are concerned with maintaining a fixed history of measurements for display upon request, and with using collections of measurements to predict an impending failure. These two methods of trend analysis are described as follows:

- Data Collection - Gather raw data from selected test points and store on an as-requested basis. The quantity of data retained is limited to a pre-set value, selected for each particular test point. The oldest measurements are dropped as new ones are obtained.

- Extrapolation - Gather data as above and perform exponential smoothing, adjustment for trend, and extrapolation after each measurement to determine if an impending out-of-limit condition exists.

In addition to the two trend analysis functions described above, the Solar Array design requires the following:

- Telemetry - Measurements obtained by this function are telemetered directly to the ground. Provision is made for temporary onboard storage, in case the telemetry link is unavailable.

The on-off cycling of certain assemblies requires that a status check be performed prior to measuring the parameter. If the assembly is inactive, the measurement is not made.

In Table 6-1 and Table 6-2, the Isotope/Brayton and Solar Array trend analysis requirements are summarized. An estimate of the auxiliary storage requirements for intermediate results may be estimated from the number of test points and the number of retained measurements. Assuming 8 bits per measurement and 32 bits per word, the I/Br auxiliary storage requirement for trend analysis is approximately 66K words compared with an SA requirement of 1476K words. These estimates include provisions for three checkpoints in the checkpoint log.

6.2.2.2 Status Monitoring

The status monitoring functions augment the continuous monitoring functions provided in hardware form by the RDAU preprocessor. Control is passed to the status monitoring functions when an RDAU limit check occurs for selected parameters.

Input consists of test point readings and their associated limits. Output consists of crew displays and fault detection indications if the status monitoring function can confirm an error detected by an RDAU. If no confirmation is obtained, a crew display indicating the fact that status monitoring was involved is provided.

Information processing for both the Isotope/Brayton and the Solar Array transmission/conditioning/distribution assembly consists of successive measurements after an out-of-limit condition has been detected by an RDAU, to determine if the parameter will remain out of limits during a pre-set number of consecutive readings. This technique is applied to most bus voltages. The flow chart in Figure 3-14 of the Task 2 Final Report depicts a module which can be used for any parameter requiring this type of status monitoring. The delay between measurements is adjustable to meet the successive sampling rates required by each application.

For selected I/Br parameters such as compressor inlet temperature and fuel capsule temperatures, measurement of parallel redundant parameters is required to distinguish between a defective transducer LRU and a true out-of-limit condition.

In addition, it is required to raise the limit checking threshold prior to passing control to the caution and warning analysis module of the checkout executive. This is done for the following in the I/Br power subsystem:

- Heat Source
  - Fuel Capsule Temperature
  - BeO Heat Sink Temperature

- Control and Monitoring
  - Speed Control Signals

6.2.2.3 Periodic Checkout

Periodic checkout functions are required to supplement the continuous monitoring performed by the RDAU hardware in order to make a quantitative evaluation of operating characteristics, and to verify the operation of inactive or standby systems.

Input consists of test point measurements, mode/status indications, the configuration table, and interactions with the crew. Output consists of stimuli, mode/status changes, configuration changes, and crew displays.

Information processing involves a variety of techniques, ranging in complexity from verifying that parameters are within limits to cycling a standby assembly through its various modes, and using it to replace an operational assembly of the same type. Limit check verification is performed as an executive service. Other periodic tests are indicated for the Isotope/Brayton power subsystem in Table 6-3, and for the Solar Array power subsystem in Table 6-4.

6.2.2.4 Fault Isolation

The fault isolation function locates the source of error which has been suggested by fault detection, status monitoring, crew/ground, periodic checkout, or trend analysis. It is a goal of this function to isolate to the failed Line Replaceable Unit (LRU). The modular design of this function follows the design of the EPS itself. In Figure 6-3 through Figure 6-9, two levels of detail are presented for the Isotope/Brayton hierarchy, while the Solar Array design is shown in Figure 6-10 through Figure 6-12.

Table 6-1. Isotope/Brayton Trend Analysis

TEST POINT	NUMBER OF MEASUREMENTS	TREND METHOD	MEASUREMENT RATE	MEASUREMENTS RETAINED PER TEST POINT
SHIELD:				
Shield Drive Motor Torque	2	Data Collection	See Note 1	TBD
POWER CONVERSION SYSTEM:				
HRHX Coolant Inlet Temperature	2	Extrapolation	1/mo.	TBD
Recuperator Outlet Temperature	2	Extrapolation	1/mo.	TBD
Gas Loop Flow Rate	2	Extrapolation	1/week	TBD
GAS MANAGEMENT SYSTEM:				
Gas Storage Pressure	2	Data Collection	1/week	TBD
HEAT REJECTION SYSTEM:				
Pump Motor Current In	2	Extrapolation	1/week	52
Pump Motor Pressure Out	2	Extrapolation	1/week	52
Radiator Coolant Discharge	2	Extrapolation	1/week	52
HEAT SOURCE:				
Fuel Capsule Temperature	1	Extrapolation	1/week	52
TRANSMISSION/CONDITIONING/DISTRIBUTION:				
Alternator Feeder Currents	6	Data Collection	4/hour	1344
Source Bus Voltage	12	Extrapolation	4/day	84
Main 28 VDC Distributor Bus Voltage	4	Extrapolation	4/day	84
28 VDC Bus Tie Cable Current	1	Data Collection	4/hour	1344
28 VDC Load Bus Voltage	12	Data Collection	4/hour	1344
260 VDC Link Bus Voltage	2	Data Collection	4/hour	1344
400 Hz Square Wave Distributor Bus Voltage	6	Data Collection	4/hour	1344

Table 6-1. Isotope/Brayton Trend Analysis (Continued)

TEST POINT	NUMBER OF MEASURE-MENTS	TREND METHOD	MEASURE-MENT RATE	MEASURE-MENTS RE-TAINED PER TEST POINT
400 Hz Sine Wave Distributor Bus Voltage	6	Data Collection	4/hour	1344
Regulated Transformer-Rectifier Output Current	5	Data Collection	4/hour	1344
Regulated Transformer-Rectifier Temperature	5	Data Collection	4/day	56
High Voltage Rectifier Output Current	4	Extrapolation	4/day	64
High Voltage Rectifier Regulator Temperature	4	Extrapolation	4/day	64
400 Hz Square Wave Inverter Temperature	2	Extrapolation	4/day	64
400 Hz Sine Wave Inverter Temperature	2	Extrapolation	4/day	64
60 Hz Sine Wave Inverter Temperature	2	Extrapolation	4/day	64
Battery Charger Regulator Output Current	10	Data Collection	4/hour	1344
Battery Charger Regulator Temperature	10	Extrapolation	4/day	64
Battery Charger Regulator Rate Mode	10	Data Collection	4/hour	1344
Battery Buck Regulator Temperature	10	Extrapolation	4/day	64
Battery Terminal Voltage	10	Extrapolation	4/day	64
Battery Monitor Voltage	10	Extrapolation	4/day	64
Battery Temperature	10	Extrapolation	4/day	64

NOTE 1: The measurement rate (TBD) will apply only during periodic checkout of the shield motor.

Table 6-2. Solar Array Trend Analysis

TEST POINT	NUMBER OF MEASURE-MENTS	TREND METHOD	MEASURE-MENT RATE	MEASURE-MENTS RE-TAINED PER TEST POINT
BATTERIES:				
Battery Voltage	12	Data Collection	4/day	84
ARRAY:				
Circuit Voltage	160	Telemetry	Varies	2
Circuit Current	160	Telemetry	Varies	2
TRANSMISSION/CONDITIONING/DISTRIBUTION				
Core & Boom Inverter Power Output (3ϕ)	8	Data Collection	4/hour	1344
Core & Boom Inverter Temperature	8	Extrapolation	4/day	84
Inverter Feeder Current	12	Data Collection	4/hour	1344
Primary Bus Voltage	12	Data Collection	4/minute	78720
Primary Bus Tie Cable Current	12	Data Collection	4/minute	78720
Battery Charger Temperature	12	Extrapolation	4/day	84
Autotransformer Temperature	4	Extrapolation	4/day	84
Secondary Bus Structure Coolant Temperature(in)	4	Extrapolation	4/day	84
Secondary Bus Structure Coolant Temperature(out)	4	Extrapolation	4/day	84
Secondary Bus Structure DC Bus Voltage	4	Data Collection	4/hour	1344
Secondary Bus Structure AC Bus Voltage	12	Extrapolation	4/hour	2016
60 Hz Inverter Temperature	2	Extrapolation	4/day	84
Rectifier-Filter Temperature	4	Extrapolation	4/day	84
Rectifier-Filter Input Voltage	12	Data Collection	4/hour	1344
Rectifier-Filter Output Current	4	Data Collection	4/hour	1344

Table 6-3. Isotope/Brayton Periodic Tests

TEST NAME	NO. OF TEST APPLICATIONS	MEASUREMENTS	STIMULI	FREQUENCY
Drive Mechanisms	2	2	1	4/year
IRV System	2	6	-	4/year
Inverters	1	82	30	1/week
Battery Chargers	10	9	4	1/week
Selector Switches	TBD	TBD	TBD	1/month
Motor Generators	2	22	8	1/month
Transformer-Rectifiers	5	5	1	1/month
High-Voltage Rectifiers	4	12	2	1/month
Buck Regulators	10	6	4	1/month
Circuit Breakers	1	208	208	4/year
Contactors	TBD	TBD	TBD	4/year
Switches	1	81	81	4/year
Differential Relays	1	6	6	2/year
Reverse-Current Relays	1	18	18	2/year

Table 6-4. Solar Array Periodic Tests

TEST NAME	NO. OF TEST APPLICATIONS	MEASUREMENTS	STIMULI	FREQUENCY
60 Hz Inverters	2	7	3	1/week
Battery Chargers	18	11	2	1/week
Core & Boom Inverters	1	80	36	1/month
Rectifier-Filters	4	5	3	1/month
Power Contactors	1	88	88	4/year
Differential Protection	1	52	52	2/year
Array Circuit I-V Test	1	400	-	1/day
Battery Controls & Indicators	1	12	12	1/week
Battery Cell Recondition Signals	1	72	36	1/week
Battery Cell By-Pass	1	1800	900	1/month

Input consists of information from configuration and mode/status tables, measurements, and crew interaction. Output consists of stimuli, commands through operational interfaces, and displays.

Information processing consists of determining if interfaces to the subsystem or assembly are being properly supplied, followed by an evaluation of the output of the assembly. If the supplied interfaces from other assemblies are within tolerance and the output is bad, the assumption is made that the fault lies within the assembly, and further analysis is made using the test points and operational interfaces associated with the assembly.

Some special fault isolation considerations which arise for the Electrical Power Subsystem are outlined as follows:

- Considered as a single assembly, the interfaces supplied to EPS are principally structural, with comparatively minor interfaces with EC/LS and DMS.
- Some of the EPS assemblies, such as the primary buses in the I/Br design, are connected together at the same hierarchical level.
- Assemblies of EPS tend to be serially interrelated, rather than parallel, as in other subsystems such as GN&C.
- In the I/Br design, transducers are specified as LRUs.

Because of the simplicity of incoming interfaces, particularly at the power conversion system level, the Electrical Power Subsystem may be used as a beginning point for integrated fault isolation at the subsystem level.

Fault isolation for assemblies which operate in closed loops may involve an intermediate interface evaluation after supplied interfaces are examined, in order to evaluate tie connections at the same assembly level. In some cases, opening the loop may be required for additional analysis. Modular concepts are also affected by closed loop operation, since a single fault isolation program module which addresses all the assemblies may be required, as opposed to a module which evaluates one assembly and is used multiple times.

The serial nature of EPS requires more extensive interface between fault isolation modules, and a deeper module nesting than would be the case for a more parallel assembly.

The specification of transducers as LRUs implies the use of calculations involving alternate measurements to ascertain whether the transducer indication is accurate. In the I/Br design, energy balance equations are employed which make use of temperature, pressure, and fluid flow to corroborate measurements obtained through transducers which are themselves line replaceable units.

6.2.2.5 Reconfiguration

The reconfiguration function maintains the portion of the configuration table as it applies to EPS. This function becomes active as a result of the removal of an assembly containing a failed LRU, or the addition of an assembly after repair.

Input consists of status and configuration data from tables and symbolic identities of the assemblies to be reconfigured. Output consists of table updates, stimuli, and commands necessary to connect or disconnect the assembly. Measurements are made to assure that the stimuli and commands have taken place.

Information processing includes the logic necessary to effect remove/replace activities with EPS assemblies, and to record the result in the configuration and status tables. Interface with operational programs such as start-up and shut-down functions are required during processing associated with the I/Br combined rotating unit. In both the SA and I/Br transmission, conditioning, and distribution modules, interface with the power management operational module is required for load balancing.

6.2.3 INTERFACE REQUIREMENTS

Although the checkout programs, language, and executive are designed to operate in a multiprocessor, there is no restriction as to the number of processors which must be available. In fact, a uniprocessor would be sufficient, provided enough main storage is available to contain the executive, program text, and data. The minimum Data Management Subsystem (DMS) configuration required for an EPS checkout function is as follows:

1 - Auxiliary Storage LRU
1 - Processor LRU
3 - Memory LRUs
1 - Data Bus Controller LRU
TBD- Data Bus Terminal LRUs
TBD- Remote Data Acquisition Unit LRUs
TBD- Stimulus Generation LRUs

This minimum configuration does not accommodate DMS failures.

The three memory LRUs are assumed to be utilized in the following manner: one for executive text, one for program text, and one for executive tables and program data. The number of RDAUs and Stimulus Generation Units (SGUs) will be determined by the function and the design details of the EPS. The number of data bus terminals is determined from the number of RDAUs and SGUs.

6.2.3.1 Interface Diagram

The relationship among the various EPS checkout functions and their means of initiation are shown in Figure 6-13.

6.2.3.2 Detailed Interface Definition

Figures 6-14 through 6-18 indicate the interface requirements for the individual functions.

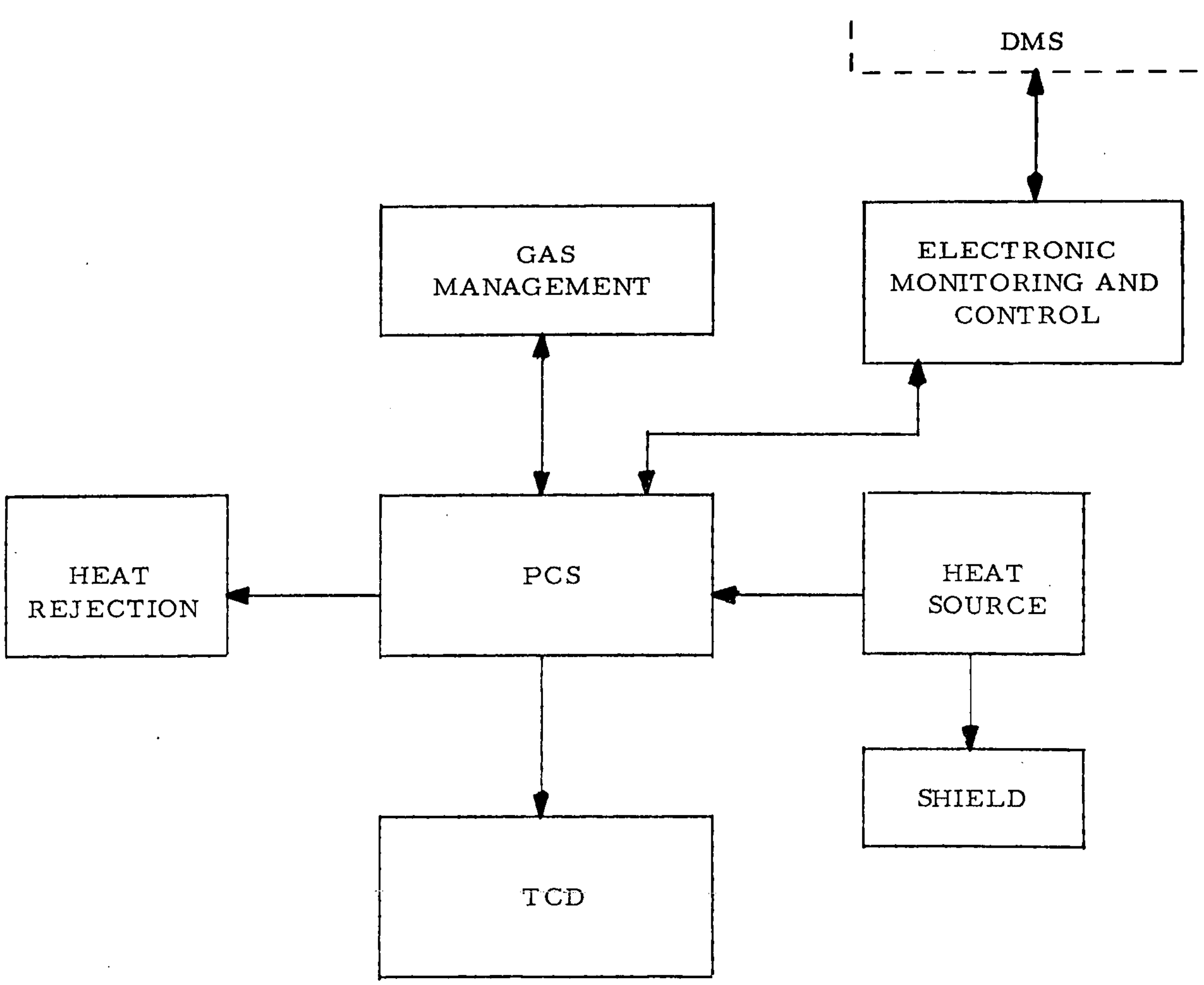
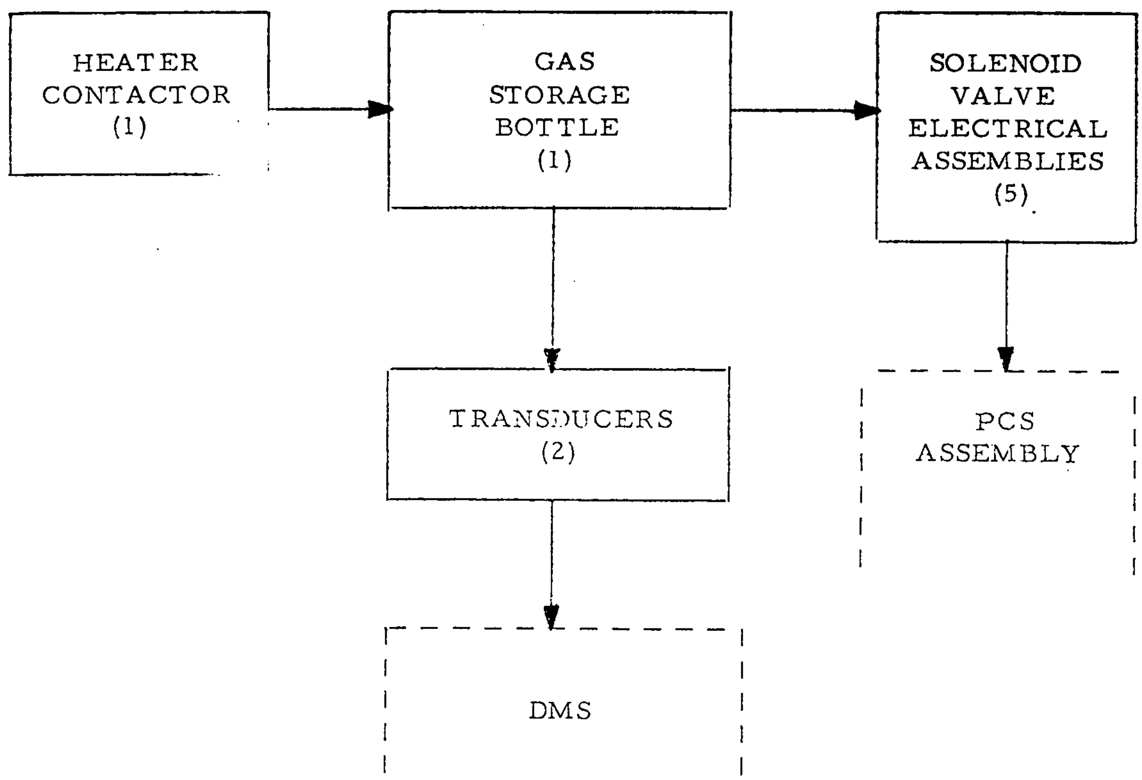
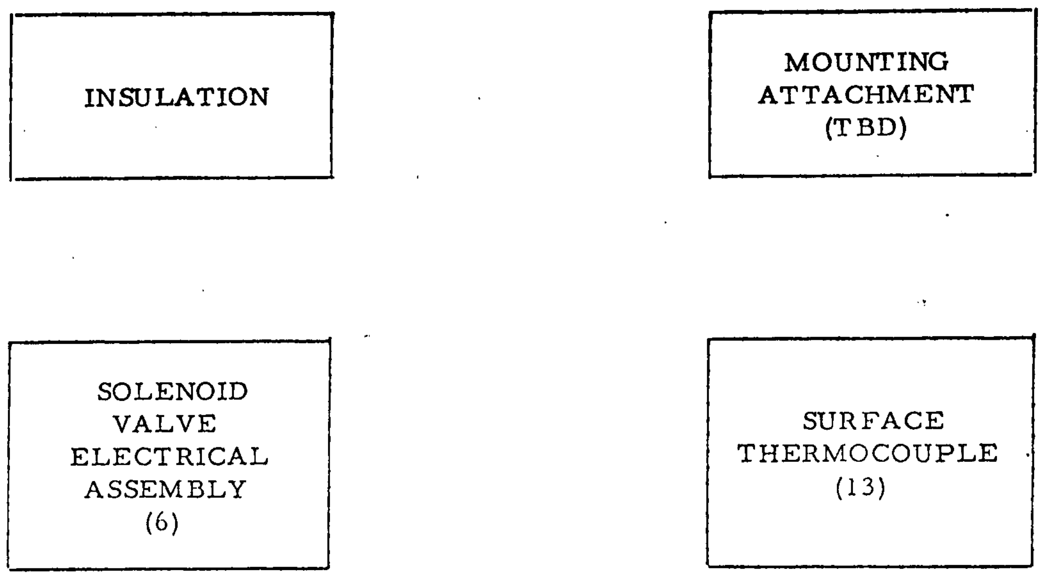


Figure 6-3. EPS Assembly Relationships, I/BR Configuration



Measurements	9	Per Assembly	Required	2
Stimuli	0		Redundant	0
LRUs	9		Total	2

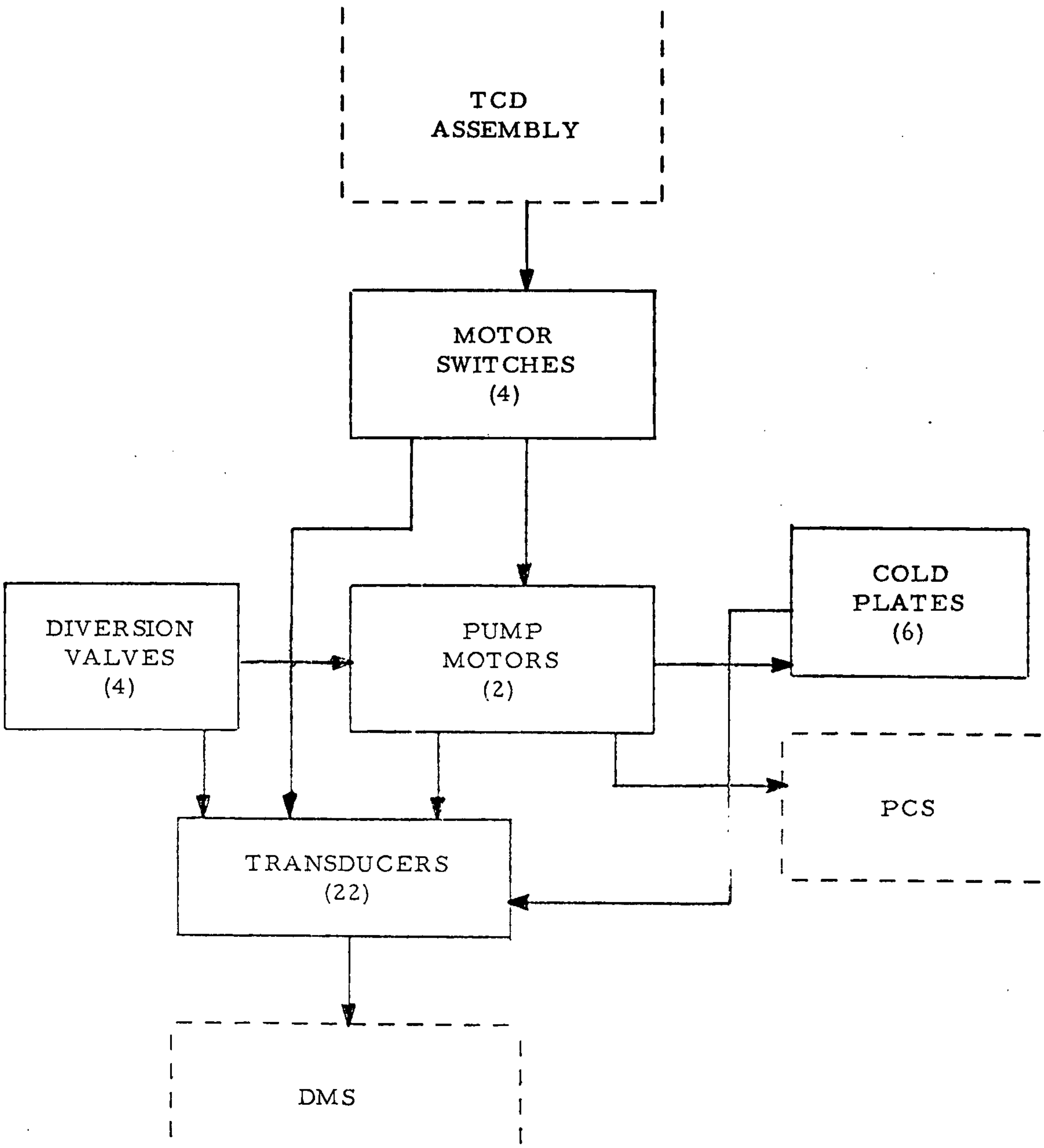
Figure 6-4. LRU Interface Diagram, Gas Management Assembly



Measurements	20	Per Assembly
Stimuli	0	
LRUs	19+TBD	

Required	2
Standby	1
Total	3

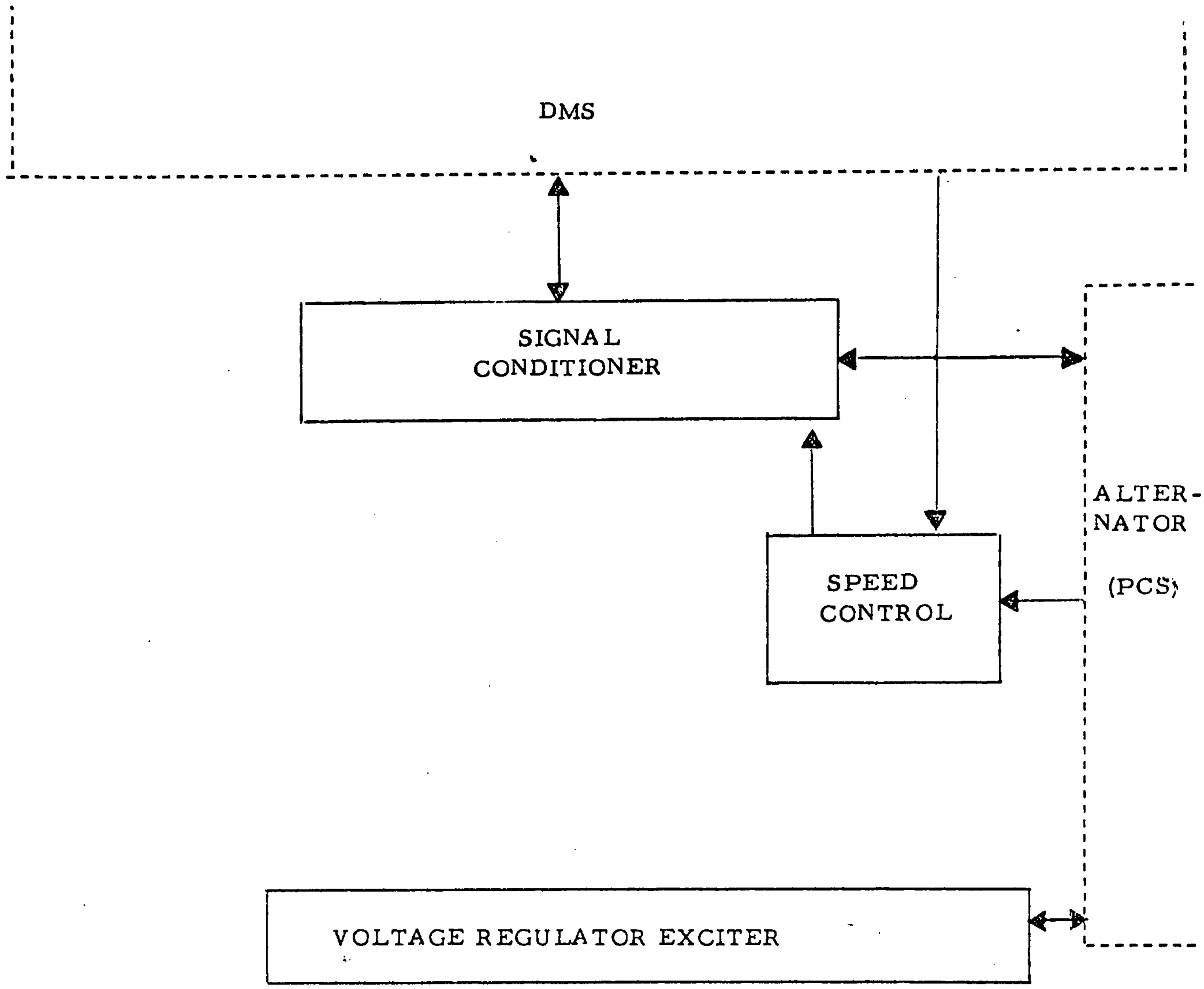
Figure 6-5. LRU Interface Diagram, Power Conversion Subsystem



Measurements	26	Per Assembly
Stimuli	0	
LRUs	38	

Required	1
Redundant	1
Total	2

Figure 6-6. LRU Interface Diagram, Heat Rejection System Assembly



Measurements	15	Per Assembly	Required	1
Stimuli	3		Redundant	1
LRU's	5		Total	2

Figure 6-7. LRU Interface Diagram, Electronic Monitoring and Control Assembly

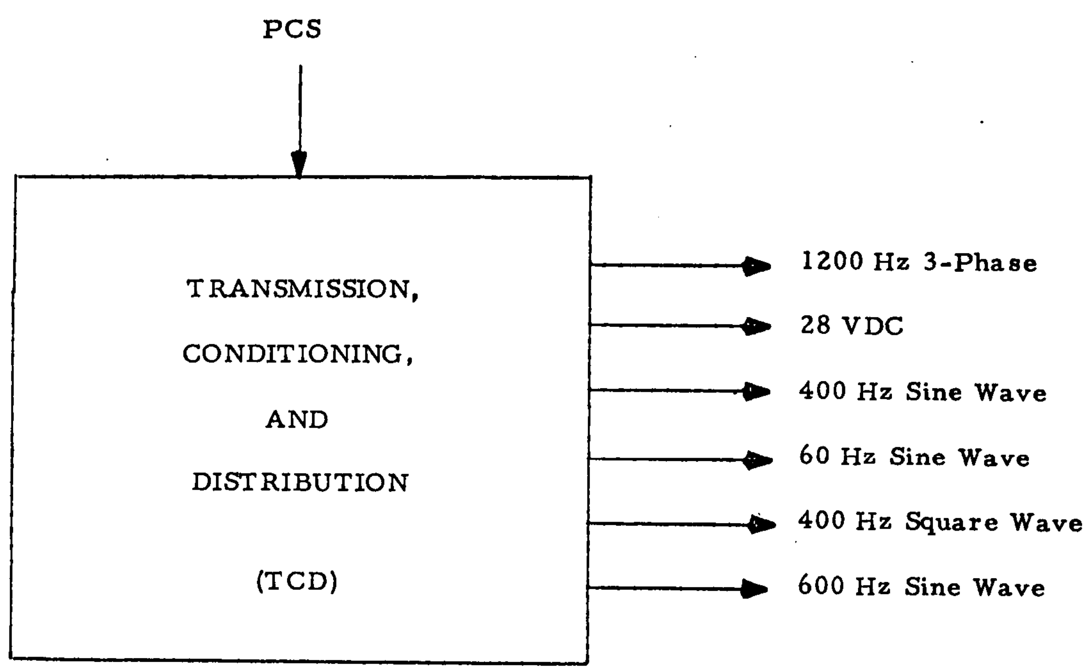
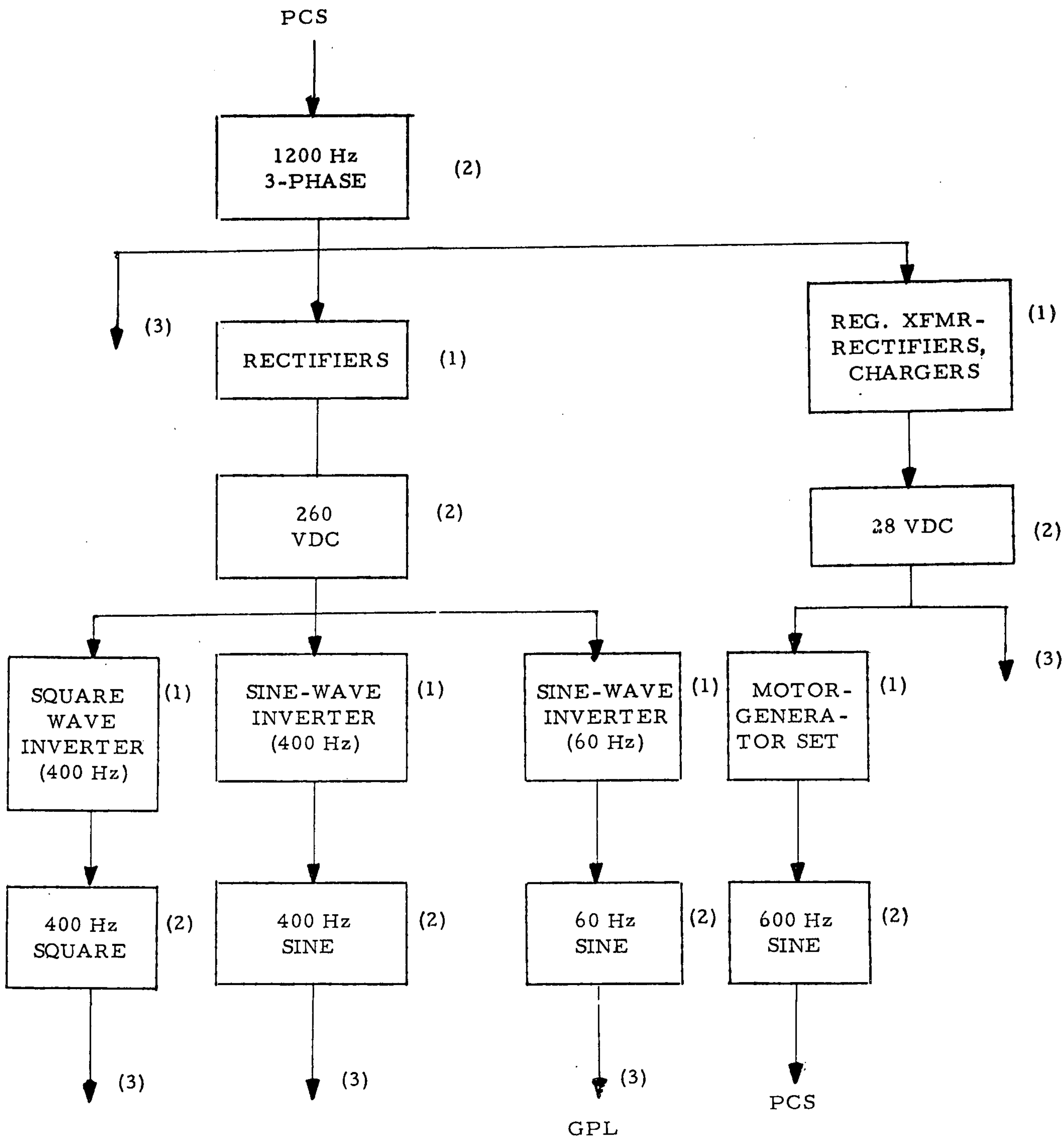


Figure 6-8. T/C/D (I/Br Configuration)



NOTES: (1) Power Conditioning Equipment
(2) Distribution and Transmission Equipment (Buses, Breakers, etc.)
(3) To the Load

Figure 6-9. Power TCD (Isotope/Brayton)

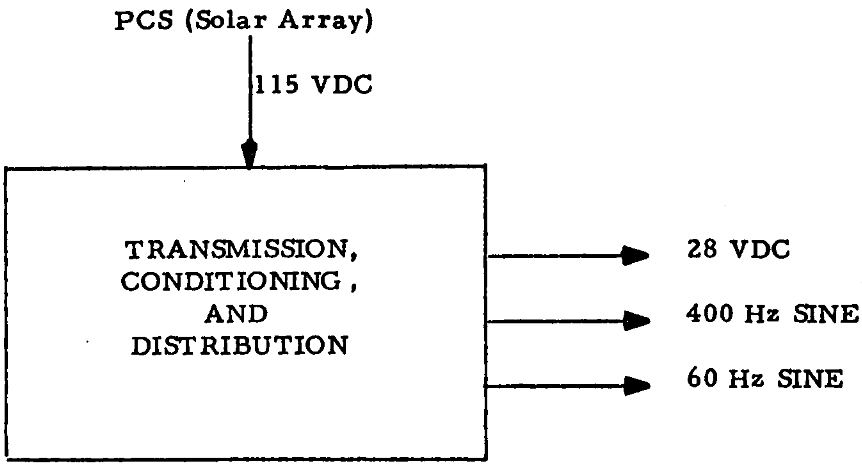


Figure 6-10. T/C/D (Solar Array Configuration)

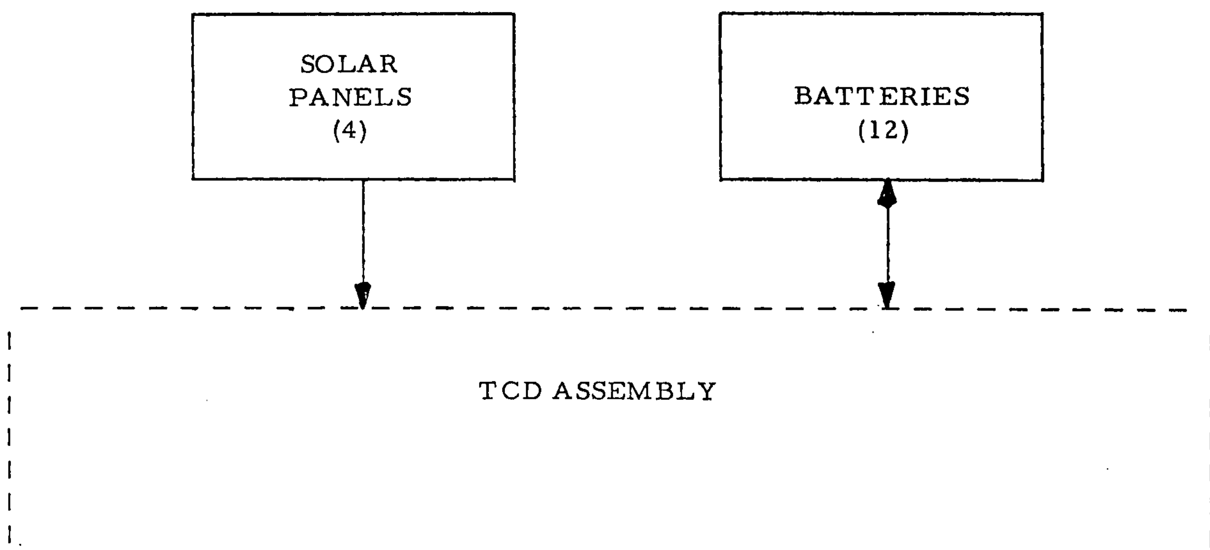


Figure 6-11. Power Source (Solar Array Configuration)

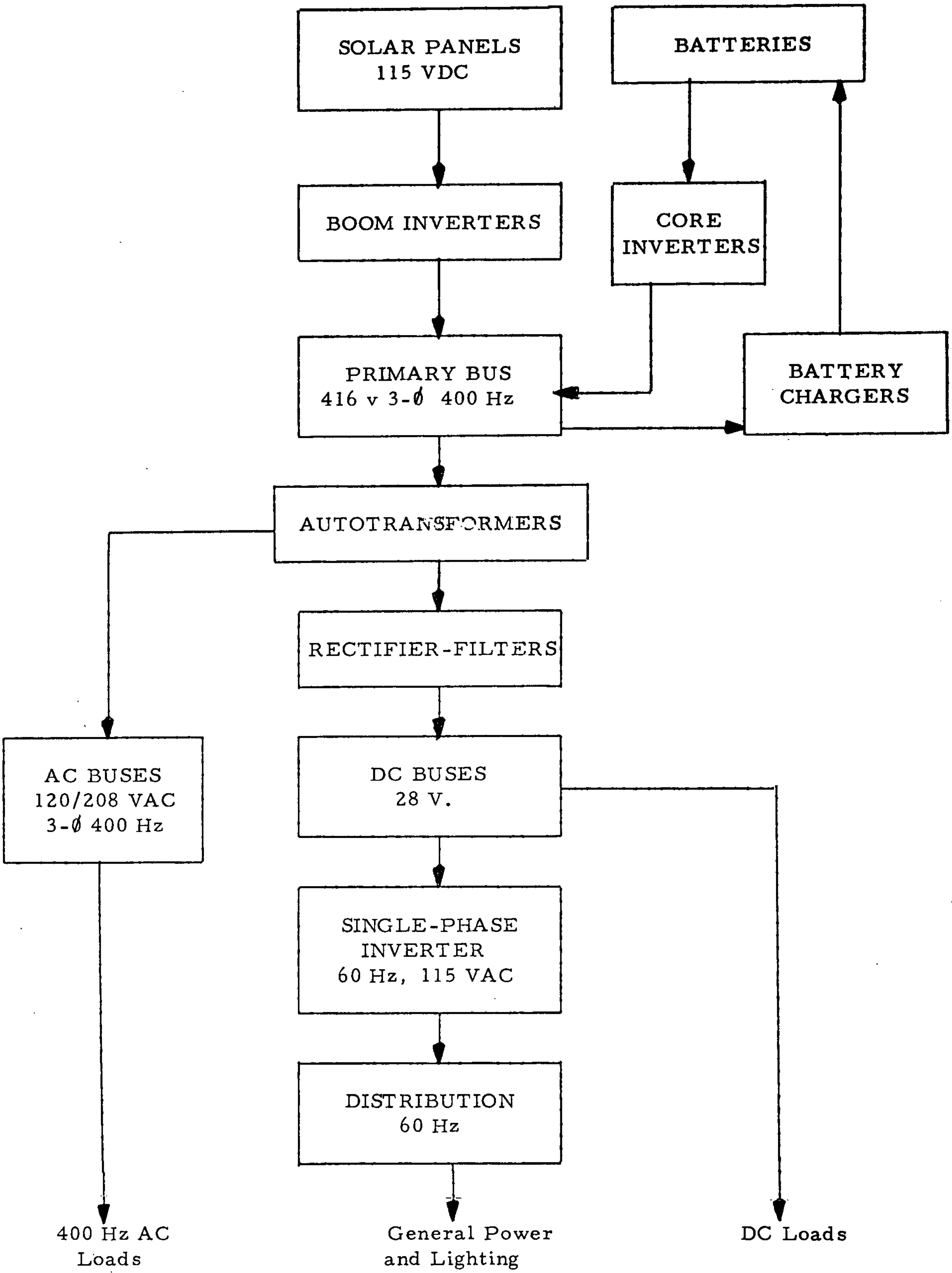


Figure 6-12. Assembly Diagram, Electrical Power Subsystem (Solar Array Configuration)

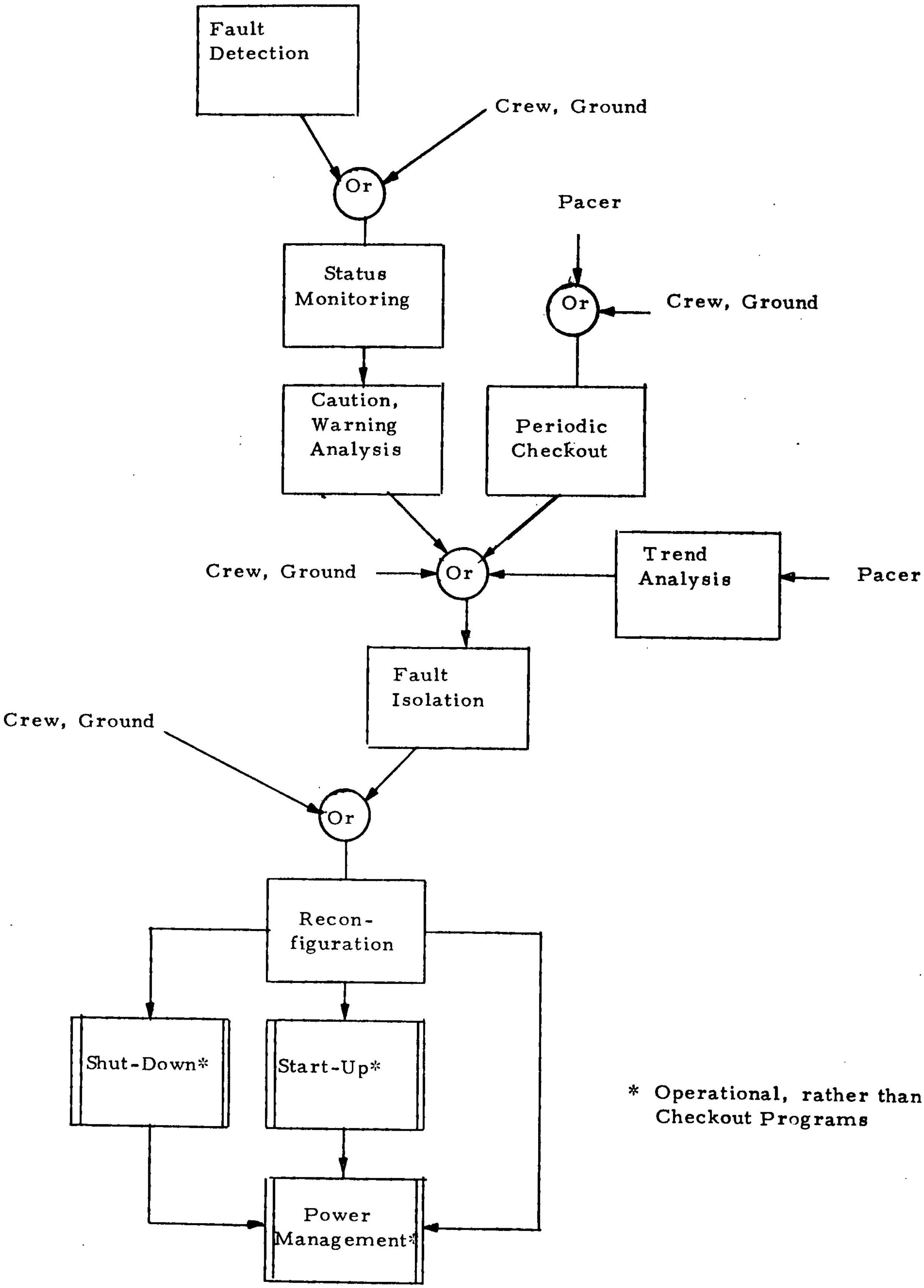


Figure 6-13. General Function Interface

(The trend analysis function receives control from an RDAU interrupt or from the Pacer.)

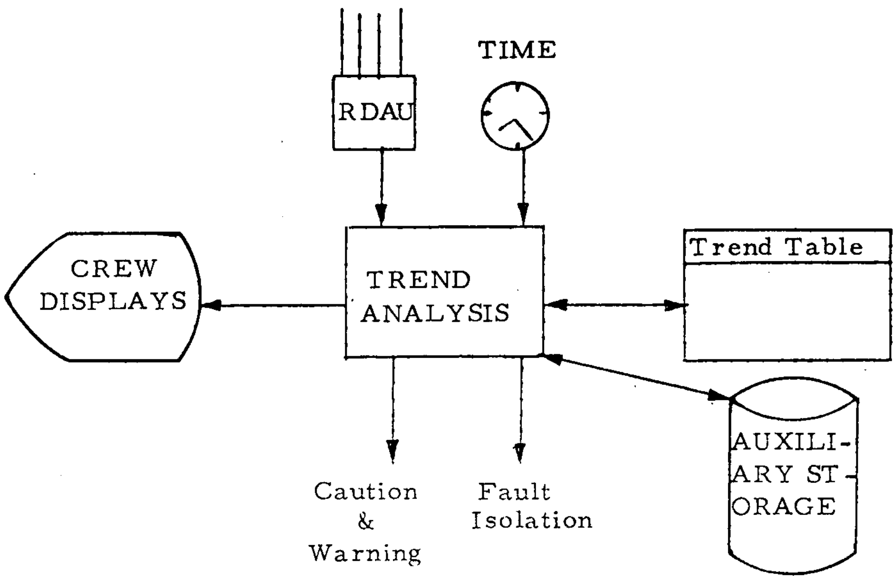


Figure 6-14. Trend Analysis Interface

(The Status Monitoring function is normally initiated by the executive as a result of an out-of-limit condition detected by an RDAU for certain selected test points. The function can also be initiated by a crew or ground).

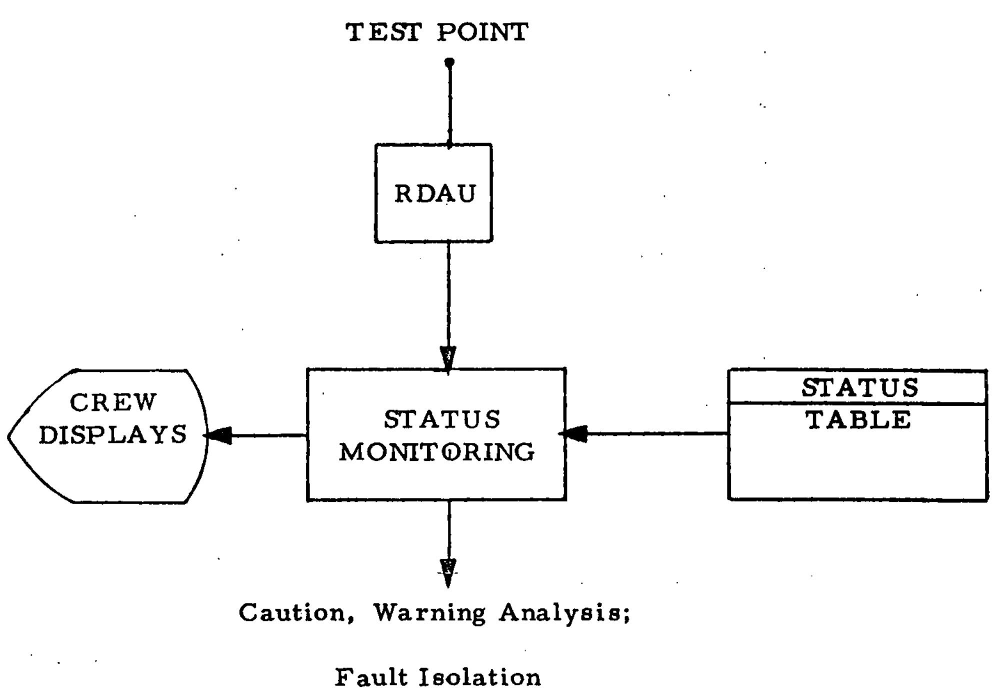


Figure 6-15. Status Monitoring Interface

(The periodic checkout function is normally initiated by the crew; however, it is possible to schedule the test automatically by utilizing the pacer (an executive service which utilizes the interval timer and a table of events)).

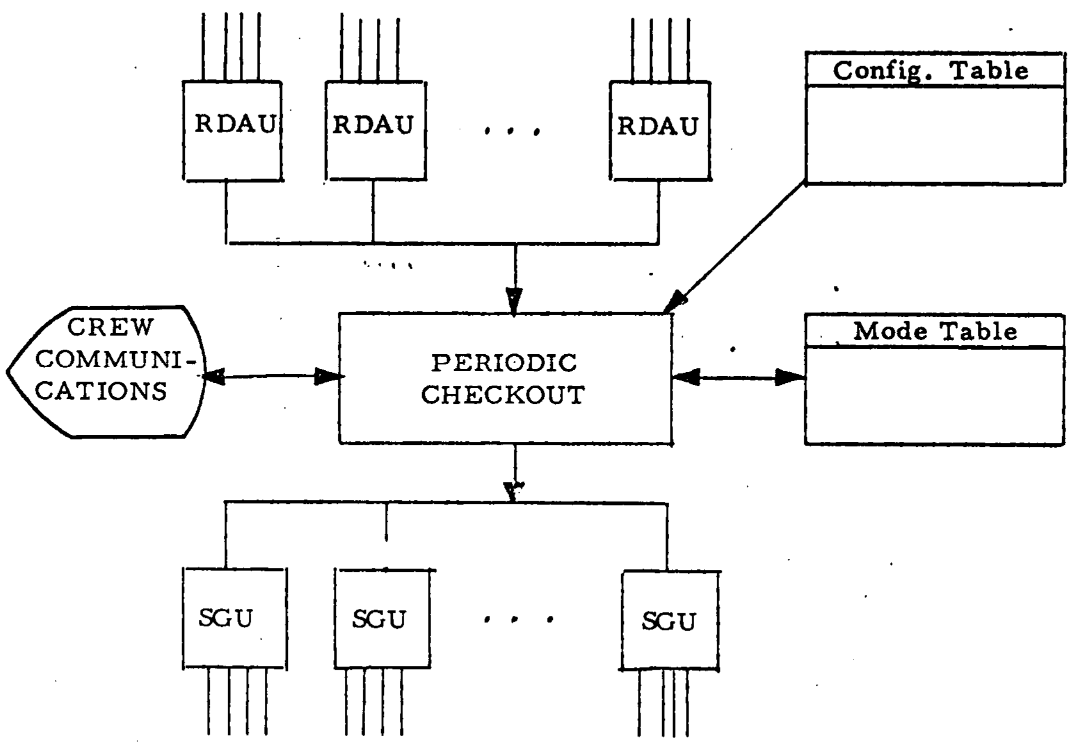


Figure 6-16. Periodic Checkout Interface

(Fault isolation modules for the EPS Subsystem receive control from the subsystem level fault isolation program and interface with the crew via the display units).

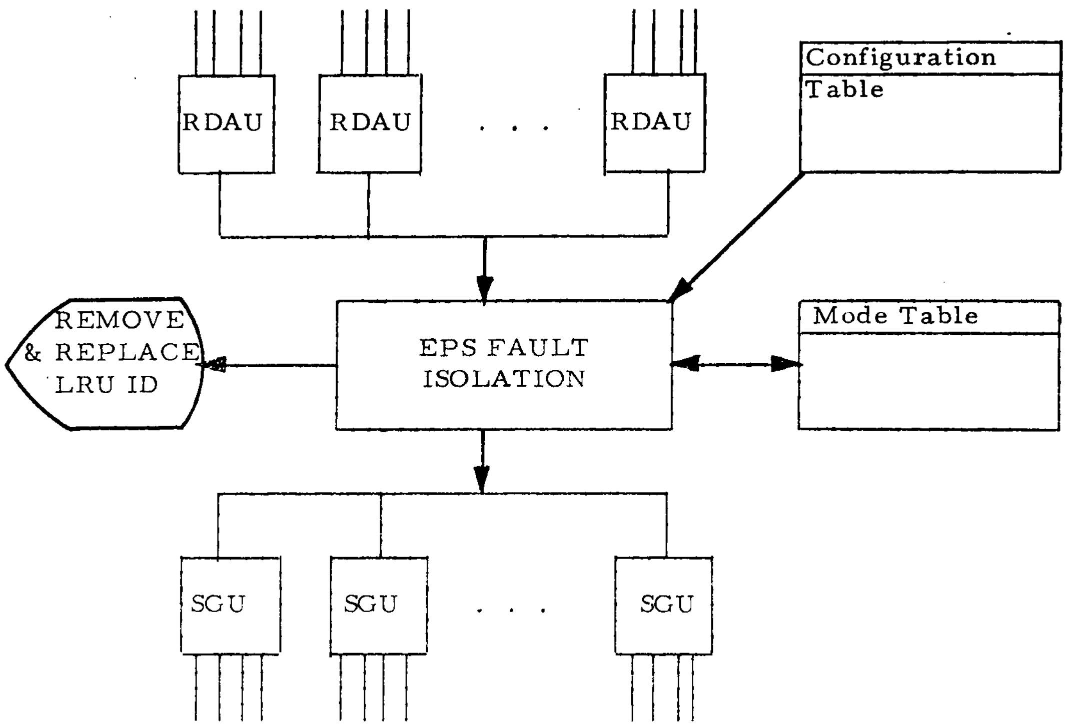


Figure 6-17. Fault Isolation Interface

(The reconfiguration function receives control from a crew command, or from the fault isolation modules).

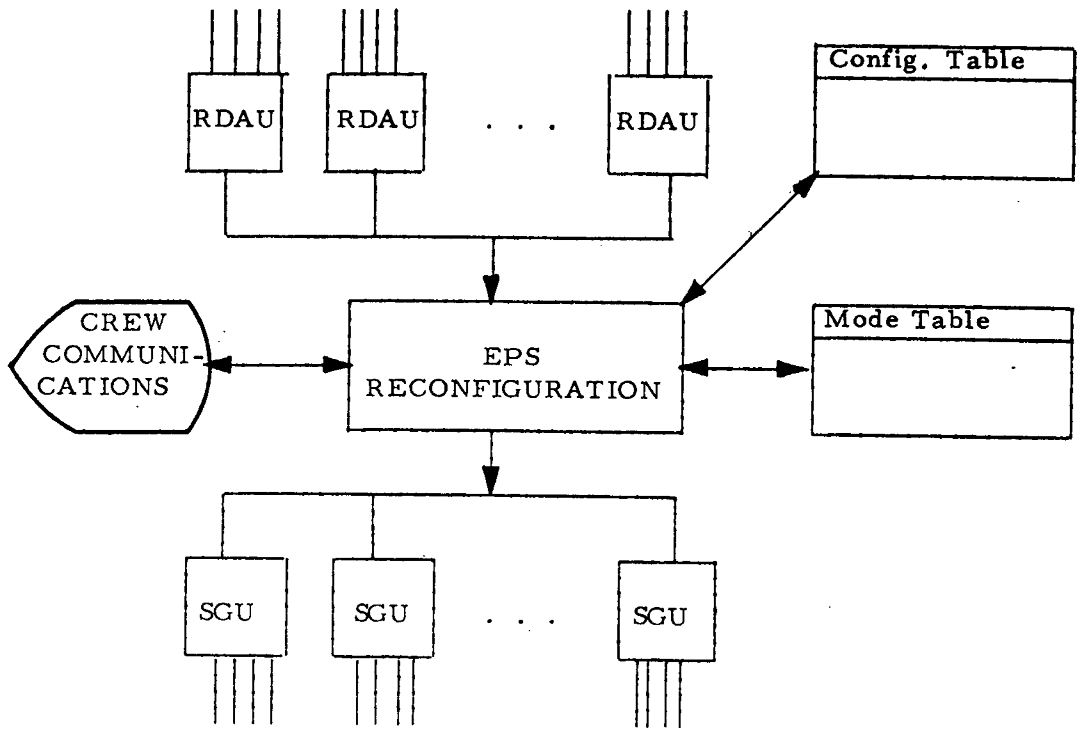


Figure 6-18. Reconfiguration Interface

Section 7

MAINTENANCE

There are two aspects of maintenance which entered into the basic study. Basic maintenance concepts were provided as part of the baseline resulting from the Phase B Space Station study; they are discussed in subsection 7.1 below. Additionally, one of the study tasks was aimed at implementation of an onboard electronics maintenance capability. The results of that task are summarized in subsection 7.2.

7.1 BASELINE MAINTENANCE CONCEPTS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment.

7.1.1 GENERAL SPACE STATION MAINTENANCE POLICY

It is a Space Station objective that all elements be designed for a complete replacement maintenance capability unless maintainability design significantly decreases program or system reliability. This objective applies to all subsystems wherever it is reasonable to anticipate that an accident, wearout, or other failure phenomenon will significantly degrade a required function. Estimates of mean-time-between-failure, or accident/failure probability, are not accepted as prima facie evidence to eliminate a particular requirement for maintenance. Should the accident/failure probability be finite, the hardware is to be designed for replacement if it is reasonable and practical to do so.

As a design objective, no routine or planned maintenance shall require use of a pressure suit [either EVA or internal vehicular activity (IVA)] . Where manual operations in a shirtsleeve environment are impractical, remote control means of affecting such maintenance or repairs should be examined. However, EVA (or pressure suit IVA) is allowable where no other solution is reasonable, such as maintenance of external equipment.

Time dependency shall be eliminated as a factor of emergency action insofar as it is reasonable and practical to do so. This includes all program aspects of equipment, operations, and procedures which influence crew actions. When time cannot be eliminated as a factor of emergency action, a crew convenience period of 5 minutes is established as the minimum objective. The purpose of the convenience period is to provide sufficient time for deliberate, prudent, and unhurried action.

7.1.2 ONBOARD MAINTENANCE FACILITY CONCEPTS

In addition to OCS/DMS capabilities, other onboard maintenance support facilities provided on the Space Station include:

- Special tools for mission-survival contingency repairs such as soldering, metal cutting, and drilling, as determined from contingency maintenance analyses, although repairs of this type are not considered routine maintenance methods.

- Protective clothing or protective work areas for planned hazardous maintenance tasks (such as those involving fuels, etc.).

- Automated maintenance procedures and stock location data for both scheduled and unscheduled maintenance and repair activities.

- Real-time ground communication of the detailed procedures, update data, and procedures not carried onboard.

- Onboard cleanroom-type conditions by "glove box" facilities compatible with the level at which this capability is found to be required.

- Maintenance support stockrooms or stowage facilities for spares located in an area that provides for ease of inventory control and ready accessibility to docking locations or transfer passages.

7.1.3 SUBSYSTEM MAINTENANCE CONCEPTS

Space Station subsystems utilize modular concepts in design and emplacement of subsystem elements. Subsystem modularity enhances man's ability to maintain, repair, and replace elements of subsystems in orbit. Providing an effective onboard repair capability is essential in supporting the Space Station's ten-year life span since complete reliance on redundancy to achieve the long life is not feasible. The need for a repair capability, in turn, requires that a malfunction be isolated to at least its in-place remove-and-replace level. The level of fault isolation is keyed to the LRU, which is the smallest modular unit suitable for replacement. The identification of subsystem LRUs is addressed as a separate, but interdependent, part of the Onboard Checkout Study.

Specific subsystem maintenance concepts, of course, depend upon examination of the subsystems. These concepts are discussed in subsequent subparagraphs. General subsystem-related maintenance guidelines that have been established for the Space Station are:

- It is an objective to design so that EVA is not required. However, EVA may be used to accomplish maintenance/repair when no other solution is reasonable.

- Subsystems will be repaired in an in-place configuration at a level that is acceptable for safety and handling, and that can be fault-isolated and reverified by the integrated OCS/DMS. This level of maintenance is referred to as line maintenance and the module replaced to effect the repair is the LRU.

- A limited bench-level fault isolation capability will be provided on the Space Station, but is only intended for contingency (recovery of lost essential functions beyond the planned spares level) or for development purposes. Limited bench-level support is also provided in the form of standard measurement capabilities which are used primarily to reduce the amount of special test equipment required.

- Subsystem elements, wherever practical, will be replaced only at failure or wearout. Limited-life items that fail with time in a manner that can be defined by analysis and test will be allowed to operate until they have reached a predetermined level of deteriorated performance prior to replacement. Where subsystem downtimes for replacement or repair exceed desirable downtimes, the subsystem will include backup (redundant) operational capability to permit maintenance. Expendable items (filters, etc.) will be replaced on a preplanned, scheduled basis.

7.2 ONBOARD ELECTRONIC MAINTENANCE (STUDY TASK 3)

The objective of this task was to generate recommendations of supporting research and technology activities leading to implementation of a manned electronics maintenance facility for the Space Station. Early in the task it became apparent that attention could not be confined to a central maintenance facility; it was necessary to refocus the task to address implementation of an on-board maintenance capability encompassing in-place as well as centralized maintenance activities. The critical questions are the following:

- What is the optimum allocation of onboard maintenance functions between in-place and centralized maintenance facility locations?

- What is the optimum level of onboard repair (i.e., to line-replaceable unit, subassembly or module, piece part, or circuit element)?

7.2.1 MAINTENANCE CYCLE

In order to place the task in the proper context, a generalized Space Station electronic maintenance cycle is depicted in Figure 7-1.

A convenient place to enter the cycle is with detection of a fault ("In-Place Maintenance" block). The fault is isolated to a Line Replaceable Unit (LRU). The affected subsystem is restored to full capability by replacing the failed LRU with an operable one from spares storage.

The failed LRU is taken to a maintenance facility (assumed for the moment to have a fixed location in the Space Station) where it is first classified as repairable or non-repairable. Classifications will likely be predetermined, and a listing should be retained in the Data Management Subsystem. If the LRU is non-repairable, it is placed in segregated storage. If the LRU is repairable on board, the fault is further isolated to the failed Shop Replaceable Assembly (SRA). The LRU is then repaired by replacing the failed SRA with one from spares storage. The repaired LRU is then calibrated (if necessary), and its operation verified before it is placed in spares storage.

Logistics requirements (replacement LRUs and SRAs needed) are transmitted to ground-based logistics support functions by RF communications and/or Space Shuttle. Failed units are taken away from and replacement units are delivered to the Space Station by the Space Shuttle.

7.2.2 SUMMARY OF RESULTS

The study confirmed and emphasized the necessity of onboard maintenance for any manned mission of any complexity and duration measured in months (up to 10 years for Space Station). Formulation of recommendations for implementing such a capability required consideration of other topics first, and achievement of certain interim results. The principal conclusions of this study task are summarized below. The analyses leading to them are explained in the Task 3 Final Report.

- Prior studies and developments of in-space maintenance have emphasized justification of first-level (in-place) maintenance, fasteners, and tools for space application and human factors criteria. Much less attention has been devoted to test equipment, maintenance training, or definition of shop level maintenance requirements.

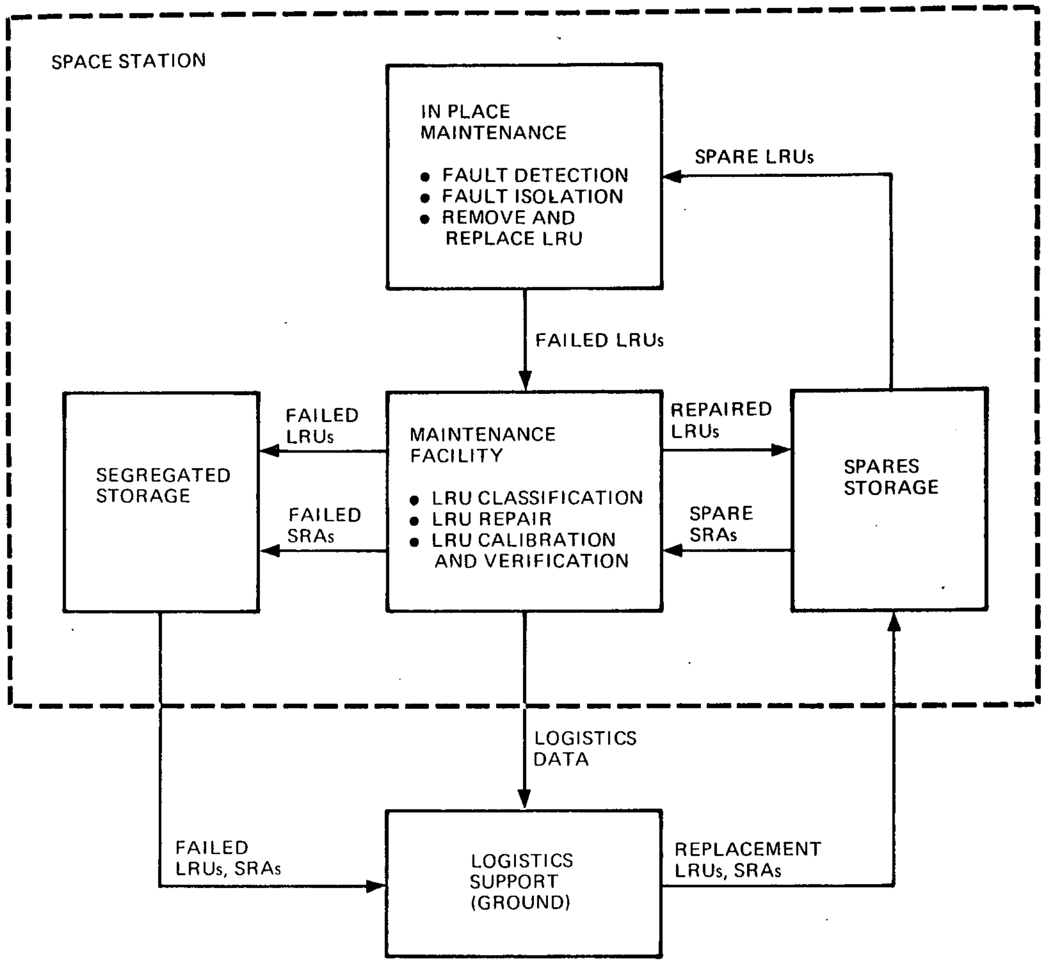


Figure 7-1. Space Station Maintenance Cycle

- The baseline subsystem descriptions, checkout requirements analysis, and software requirements analysis indicate that approximately 60 percent of all faults (over a long period) can be isolated to the failed LRU automatically under software control, without crew intervention. In an additional 27 percent of failure cases, fault isolation to one LRU can be achieved by the crew using the onboard Data Management System as a tool. In the remaining failure cases, additional fault isolation capabilities are needed. This is a good result for a "first iteration" and can probably be improved considerably with a modest effort to modify stimulus and measurement provisions.

- Crew involvement in scheduled and unscheduled maintenance (including participation in fault isolation) is estimated to average 7.2 manhours per week over the total mission time. This estimate is most sensitive to equipment reliability and levels at which onboard repair is performed. It is affected little by the efficiency of automated fault isolation under control of the Data Management Subsystem (DMS).

- The recommended approach to maintenance in the baseline Space Station is in-place removal and replacement of LRUs, without attempts to repair LRUs onboard, if the resupply interval is less than nine months. Onboard spares should be LRUs.

- For long resupply intervals or non-resupplied missions (as in a manned interplanetary mission), in-place maintenance should be by removal and replacement of LRUs. Repair of LRUs should be by removal and replacement of Shop Replaceable Assemblies (SRAs). Onboard spares should be SRAs.

- The Earth-orbital Space Station should include provision for development of onboard maintenance capability and techniques applicable to long duration non-resupplied missions and/or the larger, more complex Space Base.

- The baseline subsystem descriptions are at such a level of detail that precise specification of onboard tools and test equipment is neither feasible nor desirable. Anticipated needs identified qualitatively in the study are: (1) a portable test module to supplement software fault isolation as well as to assist mechanical adjustments and calibrator, (2) hand tools for removal and replacement of electronic assemblies, (3) devices for transporting and positioning spare assemblies, and (4) a central maintenance/repair bench.

- Several tasks have been identified and recommended for future performance, as part of a system study/design program or as separate supporting research and technology tasks. The principal ones deal with (1) development of a portable test assembly, (2) development of a repair/test bench with special provisions for small parts retention and for debris collection, (3) design for accessibility of test points and subassemblies, and (4) devices for transporting equipment within the Space Station.

The foregoing conclusions apply to the Modular Space Station as well as the 33-foot diameter, four-deck configuration.

The results of the study rest upon several assumptions and estimates, derived wherever possible from related experience. The results are not sensitive to small variations of the assumed or estimated values, except for equipment failure rates, which are most influential. Furthermore, it has not been practicable to pursue all trade analyses to include all relevant factors. Nevertheless, the study has generated valid insights into Space Station onboard maintenance and useful visibility of the path to implementation of that capability.